QA
26
T7-6

TRANSACTIONS

OF THE

AMERICAN MATHEMATICAL SOCIETY

EDITED BY

ELIAKIM HASTINGS MOORE

ERNEST WILLIAM BROWN THOMAS SCOTT FISKE

WITH THE COÖPERATION OF

EDWARD BURR VAN VLECK HENRY SEELY WHITE

CHARLES LEONARD BOUTON LEONARD EUGENE DICKSON JOHN IRWIN HUTCHINSON

EDWARD KASNER EDWIN BIDWELL WILSON

PUBLISHED QUARTERLY BY THE SOCIETY
WITH THE SUPPORT OF

YALE UNIVERSITY
COLUMBIA UNIVERSITY
WESLEYAN UNIVERSITY
HAVERFORD COLLEGE
THE UNIVERSITY OF MISSOURI
NORTHWESTERN UNIVERSITY
CORNELL UNIVERSITY
THE UNIVERSITY OF CALIFORNIA
THE UNIVERSITY OF CHICAGO
STANFORD UNIVERSITY

VOLUME 6
1905

LANCASTER, PA., AND NEW YORK
THE MACMILLAN COMPANY
AGENTS FOR THE SOCIETY
1905

2.

ON THE LINEAR TRANSFORMATIONS OF A QUADRATIC FORM INTO ITSELF*

BY

PERCEY F. SMITH

The problem of the determination † of all linear transformations possessing an invariant quadratic form, is well known to be classic. It enjoyed the attention of EULER, CAYLEY and HERMITE, and reached a certain stage of completeness in the memoirs of FROBENIUS,‡ VOSS,§ LINDEMANN‖ and LOEWY.¶ The investigations of CAYLEY and HERMITE were confined to the general transformation, FROBENIUS then determined all proper transformations, and finally the problem was completely solved by LINDEMANN and LOEWY, and simplified by VOSS.

The present paper attacks the problem from an altogether different point, the fundamental idea being that of building up any such transformation from simple elements. The primary transformation is taken to be *central reflection* in the quadratic locus defined by setting the given form equal to zero. This transformation is otherwise called in three dimensions, point-plane reflection,—point and plane being pole and polar plane with respect to the fundamental quadric. In this way, every linear transformation of the desired form is found to be a product of central reflections. The maximum number necessary for the most general case is the number of variables. VOSS, in the first memoir cited, proved this theorem for the general transformation, assuming the latter given by the equations of CAYLEY. In the present paper, however, the theorem is derived synthetically, and from this the analytic form of the equations of transformation is deduced.

* Presented to the Society December 29, 1903. Received for publication, July 2, 1904.

† The results of §§ 1, 2 were communicated to the American Mathematical Society in December, 1901.

‡ FROBENIUS, *Ueber linear substitutionen und bilinear Formen*, Crelle, vol. 84 (1878), pp. 1–63.

§ VOSS, *Zur theorie der orthogonalen substitutionen*, Mathematische Annalen, vol. 13 (1878), pp. 320–374; *Ueber die cogrediente Transformation der bilinearen formen in sich selbst*, Münchener Berichte (1896), pp. 1–23.

‖ LINDEMANN, *Vorlesungen über Geometrie*, vol. 2 (1891), p. 356; *Ueber die linearen Transformationen einer quadratischen Mannigfaltigkeit in sich*, Münchener Berichte (1896), pp. 31–66.

¶ LOEWY, *Ueber die Transformationen einer quadratischen Form in sich selbst*, Leop. Nova Acta, Halle, vol. 65 (1896), pp. 1–66.

The theory of central reflections developed in § 1 is so simple, and the analytic representation derived therefrom so direct that the present discussion presents a complete solution of the problem which may be regarded as elementary. Furthermore, the equations (24) found in explicit form for every such transformation have not been given elsewhere, as far as the author's knowledge goes.

In §§ 5, 6 are given some applications, and in § 7 the solution of the corresponding problem for the alternating bilinear form. The results of the first six sections apply, of course, to the symmetrical bilinear form.

§ 1. *The theory of central reflections.*

Let

$$f(x) = \sum a_{ik}x_i x_k, \qquad a_{ik} = a_{ki} \qquad (i, k = 1, 2, \cdots, n), \tag{1}$$

be the given quadratic form. The quadratic locus $f(x) = 0$ in linear space R_{n-1} of $n-1$ dimensions may be called after Cayley the "absolute." Any group of r independent sets of coördinates

$$(a_1^{(1)}, a_2^{(1)}, \cdots, a_n^{(1)}), \ \cdots, \ (a_1^{(r)}, a_2^{(r)}, \cdots, a_n^{(r)}),$$

determine a linear manifold M_{n-r-1} of $n-r-1$ dimensions, the coördinates x of any point of which are linearly derived from the a's:

$$x_i = \lambda^{(1)}a_i^{(1)} + \lambda^{(2)}a_i^{(2)} + \cdots + \lambda^{(r)}a_i^{(r)} \qquad (i = 1, 2, \cdots, n).$$

The involutory transformation which forms the basis of the discussion is the "central reflection" of Voss (loc. cit.), or the point-plane reflection, as it is often called, point and plane standing in the relation of pole and polar with respect to $f(x) = 0$. I shall denote by $\{\mathbf{a}\}$ the reflection in the point a and its polar plane, and by $x\{\mathbf{a}\}x'$ the fact of x transforming into x', from which also, since the transformation is involutory, will follow $x'\{\mathbf{a}\}x$. From the definition of the transformation x', x and a are collinear, hence $x' = x + \lambda a$, and since by hypothesis, $f(x') \equiv f(x)$, we find for the equations of $\{\mathbf{a}\}$

$$x' = x - \frac{2f(x, a)}{f(a)}a, \qquad \text{or} \qquad x = x' - \frac{2f(x', a)}{f(a)}a, \tag{2}$$

where, of course, $f(a) \neq 0$ (and may be taken equal to 1 when desired), because *the center a must not lie on the absolute.*

Evidently the center a and each point in the polar M_{n-2} of a, viz., $f(x, a) = 0$ are invariant under $\{\mathbf{a}\}$.

The product $\{\mathbf{ab}\}$ of two reflections $\{\mathbf{a}\}$ and $\{\mathbf{b}\}$ comes out as

$$x' = x - \frac{2f(x, a)}{f(a)}a - \frac{2f(x, b)}{f(b)}b + \frac{4f(x, a)f(a, b)}{f(a)f(b)}b. \tag{3}$$

This is symmetrical in a and b when and only when $f(a, b) = 0$, i. e., we have the result:

Two central reflections $\{\mathbf{a}\}$ *and* $\{\mathbf{b}\}$ *are commutative, when and only when* a *and* b *are conjugate points with respect to the absolute.**

The important question is now this: *When is* $\{\mathbf{ab}\} \equiv \{\mathbf{cd}\}$*?*

A *necessary* condition is expressed in

THEOREM 1. *If* $\{\mathbf{a}^{(1)}\mathbf{a}^{(2)}\mathbf{a}^{(3)}\cdots\mathbf{a}^{(r)}\} \equiv \{\mathbf{b}^{(1)}\mathbf{b}^{(2)}\mathbf{b}^{(3)}\cdots\mathbf{b}^{(r)}\}$*, then each of the centers* b *is numerically derived from the centers* $a^{(1)}, a^{(2)}, \cdots, a^{(r)}$.†

Take $r = 2$. Then from (3), $\{\mathbf{ab}\} \equiv \{\mathbf{cd}\}$ gives as a necessary and sufficient condition

$$(4)\quad \frac{f(x,a)}{f(a)}a + \left(\frac{f(x,b)}{f(b)} - \frac{2f(x,a)f(a,b)}{f(a)f(b)}\right)b \equiv \frac{f(x,c)}{f(c)}c + \left(\frac{f(x,d)}{f(d)} - \frac{2f(x,c)f(c,d)}{f(c)f(d)}\right)d$$

for every value of x. If $c \not\equiv a$, take $f(x,c) = 0$, and $f(x,a) \neq 0$. Then d is numerically derived from a and b. Similarly for c.

The following proof involving the principles of GRASSMANN's *Ausdehnungslehre*‡ is general and very direct. Regarding a, b, c, d as extensive magnitudes or complex quantities, and the coefficients in (4) as scalars, we notice that the coefficient of b is of the same form as that of a diminished by a multiple of the latter. Now write down (4) with x replaced by x', and multiply the corresponding members of the two equations together using the "combinatorial law" $ab = -ba$, $cd = -dc$; then, taking $f(a) = f(b) = f(c) = f(d) = 1$, we get easily

$$\begin{vmatrix} f(x,a) & f(x,b) \\ f(x',a) & f(x',b) \end{vmatrix} ab \equiv \begin{vmatrix} f(x,c) & f(x,d) \\ f(x',c) & f(x',d) \end{vmatrix} cd,$$

in which the scalar coefficients are determinants. In this form the theorem follows at once, and as the method is in no wise different for the general case, the truth of the proposition is established.

It is now necessary to add only the following theorem, after which a complete theory of central reflections may be developed by synthesis.

THEOREM 2. *The product* $\{\mathbf{ab}\}$ *of two central reflections may be resolved in* ∞^1 *ways into* $\{\mathbf{cd}\}$*, the centers* c *and* d *lying on the manifold* M_1 *derived from* a *and* b*. Either* c *or* d *may be chosen arbitrarily on this line. The other is then uniquely determined.*

For if $f(a) = 1, f(b) = 1$, and $\lambda^2 + \mu^2 + 2\lambda\mu f(a,b) = 1$, then $\{\mathbf{ab}\} \equiv \{\mathbf{cd}\}$ if $c = \lambda a + \mu b$, and $d = -\mu a + [\lambda + 2\mu f(a,b)]\,b$, as direct substitution in

* VOSS, loc. cit., p. 345.

† We assume $r \geqslant n$, and $a_1, a_2, \cdots, a_r$ independent.

‡ *Ausdehnungslehre* von 1862, p. 42.

(4) will show.* Furthermore, we cannot write $\{\mathbf{ab}\} \equiv \{\mathbf{cd}\} \equiv \{\mathbf{cd}'\}$ unless $\{\mathbf{d}\} \equiv \{\mathbf{d}'\}$. For $\{\mathbf{ccd}\}$ would in this case be identical with $\{\mathbf{ccd}'\}$, and since $\{\mathbf{cc}\}$ is the identical transformation, we must also have $\{\mathbf{d}\} \equiv \{\mathbf{d}'\}$.

The invariant configuration of $\{\mathbf{ab}\}$ is made up of the points of intersection of the line ab with the absolute, and every point of the M_{n-3} common to the two polar manifolds M_{n-2} of a and b.†

It is to be noted also that $\lambda a + \mu b$ lies upon the absolute when

$$\lambda^2 + \mu^2 + 2\lambda\mu f(a, b) = 0,$$

which is the condition of coincidence of c and d, i. e., in the resolution of $\{\mathbf{ab}\}$ the express hypothesis made in (2) that a center shall not lie upon the absolute is equivalent to coincidence of c and d.

Pass on now to $r = 3$, and the proof of

THEOREM 3. *The product of three central reflections* $\{\mathbf{abc}\}$ *may always be resolved in* ∞^3 *ways into* $\{\mathbf{def}\}$. *The first center is any point in the plane of* a, b, c; *but the line joining* e *and* f *is then uniquely determined, though either* e *or* f *may be chosen at will upon this line.*

Given, then, the three centers a, b, c, and any center d in their plane. If the point b' of intersection of ad and bc is not on the absolute, then by theorem 2, $\{\mathbf{abc}\} \equiv \{\mathbf{ab'c'}\} \equiv \{\mathbf{def}\}$. Suppose, however, $f(b') = 0$, and let a' be any center on ab, so that we may write $\{\mathbf{ab}\} \equiv \{\mathbf{a'b'}\}$. Then the lines da' and cb' are projectively related, and accordingly their point of intersection b'' describes a conic containing d and c. Since d and c are not on the absolute, this conic cannot be the intersection of the plane of centers with the absolute, and b'' may be assumed a center. Hence we now have $\{\mathbf{abc}\} \equiv \{\mathbf{a'b'c}\} \equiv \{\mathbf{a'b''c'}\} \equiv \{\mathbf{def}\}$, and the first part of theorem 3 is proved.

For the rest, if $(\mathbf{def}) \equiv (\mathbf{de'f'})$, then $(\mathbf{ef}) \equiv (\mathbf{e'f'})$ and the second part follows at once from theorem 2.

It appears, therefore, that the transformation $\{\mathbf{abc}\}$ establishes in the plane of centers a point-line relation between the first center d and the line ef upon which the remaining two must then lie.

This relation is a *correlation*. For if f is *any* center on ef, then $\{\mathbf{def}\} \equiv \{\mathbf{d}_1\mathbf{e}_1\mathbf{f}_1\}$; and if de and d_1e_1 intersect in d', we may write $\{\mathbf{d'e'f}\} \equiv \{\mathbf{d'e_1'f_1}\}$. Hence e' and e_1' are on ef, and e' and d' coincide with e and d respectively. Therefore as f in $\{\mathbf{def}\}$ moves along ef, the corresponding line turns around d. Hence the transformation $\{\mathbf{abc}\}$ establishes a duality $\{\Gamma\}$ in the plane of centers, such that the second and third centers lie upon the line that corresponds under $\{\Gamma\}$ to the first center. Furthermore, since

* The equations simply indicate that a, b and c, d are corresponding points of a projectivity on the line of centers and with fixed points upon the absolute.

† The line joining a and b touches the absolute when $f(a)f(b) = [f(a, b)]^2$.

$\{\mathbf{def}\} \equiv \{\mathbf{ed'f}\} \equiv \{\mathbf{efd''}\}$, f lies on the correlate of e, and finally, as the preceding shows that a point and its line under $\{\Gamma\}$ are united only when the point is on the absolute, we have

THEOREM 4. *The transformation* $\{\mathbf{abc}\}$ *establishes in the plane of centers a duality which is characteristic of the transformation. In any resolution of* $\{\mathbf{abc}\}$, *the line corresponding in this duality to any center contains the following centers of the product. Coincidence of point and line under this duality occurs when and only when the point is on the absolute.*

The generalization of this theorem is at once accomplished by complete induction. Assume, then, that theorems 3 and 4 hold for the product of any p central reflections $p < n$. Write the transformation

$$\{\mathbf{T}_{p+1}\} \equiv \{\mathbf{a}^{(1)}\mathbf{a}^{(2)}\cdots\mathbf{a}^{(p)}\mathbf{a}^{(p+1)}\} \equiv \{\mathbf{a}^{(1)}\mathbf{T}_p\}.$$

Let $b^{(1)}$ be any point in the M_p numerically derived from $a^{(1)}, a^{(2)}, \cdots, a^{(p+1)}$, and suppose the line $a^{(1)}b^{(1)}$ intersects the locus of centers of $\{\mathbf{T}_p\}$ in $a^{(0)}$. Considerations analogous to the preceding permit us to assume $a^{(0)}$ not on the absolute, and we may by hypothesis write $\{\mathbf{T}_p\} \equiv \{\mathbf{a}^{(0)}\mathbf{T}_{p-1}\}$. Since also $\{\mathbf{a}^{(1)}\mathbf{a}^{(0)}\} \equiv \{\mathbf{b}^{(1)}\mathbf{b}^{(0)}\}$, we evidently have $\{\mathbf{T}_{p+1}\} \equiv \{\mathbf{b}^{(1)}\mathbf{T}'_p\}$. The remainder of the proof follows as easily and may be omitted, the statement following.

THEOREM 5. *The transformation* $\{\mathbf{a}^{(1)}\mathbf{a}^{(2)}\cdots\mathbf{a}^{(r)}\}$ *compounded of* r *independent central reflections establishes within the* M_{r-1} *numerically derived from the centers* $a^{(1)}, a^{(2)}, \cdots a^{(r)}$, *a duality which is characteristic of the transformation. We may resolve the transformation in* $\infty^{\frac{1}{2}r(r-1)}$ *ways, the first center being any point in* M_{r-1}, *and the following limited only by the condition that the* M_{r-2} *corresponding to any one of them in the duality contains all the succeeding centers. Coincidence of point and corresponding* M_{r-2} *occurs when and only when the point is on the absolute. The transformation depends upon* $r(n-1) - \frac{1}{2}r(r-1) = \frac{1}{2}r(2n-r-1)$ *essential parameters.*

From this result we may at once state

THEOREM 6. *Any product of reflections in centers lying in an* M_{r-1} *may always be reduced to one of* r *factors or fewer. The most general transformation compounded of central reflections may therefore be reduced to one of* n *factors.*

The proof follows at once from theorem 5. For example, $\{\mathbf{a}^{(1)}\mathbf{a}^{(2)}\cdots\mathbf{a}^{(n)}\mathbf{a}\}$ may be written $\{\mathbf{b}^{(1)}\mathbf{b}^{(2)}\cdots\mathbf{b}^{(n-1)}\mathbf{a}\,\mathbf{a}\}$ or $\{\mathbf{b}^{(1)}\mathbf{b}^{(2)}\cdots\mathbf{b}^{(n-1)}\}$. For any, $\mathbf{T}_p = \{\mathbf{a}^{(1)}\mathbf{a}^{(2)}\cdots\mathbf{a}^{(p)}\}$ the polar M_{n-p-1} with respect to $f = 0$ of the locus of centers is a locus of invariant points. All remaining invariant points lie in the locus of centers.

§ 2. *On the resolution of any orthogonal transformations into central reflections.*

The quadratic form of the preceding section is now assumed to be

$$\phi(x) = x_1^2 + x_2^2 + \cdots x_n^2.$$

Let $\{\mathbf{T}\}$, defined by the equations

$$y_i = \sum_k \alpha_{ik} x_k \qquad (i, k = 1, 2, \cdots, n), \tag{4}$$

be any orthogonal transformation, i. e., $\phi(y) \equiv \phi(x)$. The question is to show that $\{\mathbf{T}\}$ is a product of central reflections. This is known to be the case for $n = 2$, for example. For if we interpret x_1 and x_2 as Cartesian rectangular coordinates in the plane, $\{\mathbf{T}\}$ is either a rotation around the origin or a reflection * in a line through the origin according as the determinant $|\alpha_{ik}|$ in (4) is 1 or -1. But in the case of a rotation, $\{\mathbf{T}\}$ is compounded of two line reflections.

Knowing, then, that the orthogonal transformation for $n = 2$ is always a product of central reflection, I shall prove the theorem true in general by establishing the truth of the proposition:

An orthogonal transformation in n variables may always be resolved into one in $n-1$ variables compounded with central reflections.†

We may assume in (4) that $\alpha_{nn} \neq 0$. For if this were the case, suppose $\alpha_{nr} \neq 0$, which must be true for some value of r. But the reflection $\{\mathbf{a}\}$ in the centre $a_1 = a_2 = \cdots = a_{r-1} = 0$, $a_r = 1$, $a_{r+1} = \cdots = a_{n-1} = 0$, $a_n = -1$, merely interchanges x_r and x_n, and, accordingly, composition of $\{\mathbf{T}\}$ and $\{\mathbf{a}\}$ will give us a transformation for which the hypothesis holds.

Now suppose $\alpha_{ns} \neq 0$. Consider a reflection $\{\mathbf{b}\}$ for which only b_s and b_r do not vanish. This has the form

$$\begin{aligned} x_k &= x'_k \qquad (k \neq s \neq n), \\ x_s &= \lambda x'_s + \mu x'_n, \\ x_n &= \mu x'_s - \lambda x'_n, \end{aligned}$$

where $\lambda^2 + \mu^2 = 1$. Then if $\lambda : \mu$ be chosen so that $\lambda\alpha_{ns} + \mu\alpha_{nn} = 0$, the compounded transformation $\{\mathbf{Tb}\}$, viz., $y_i = \sum_k \beta_{ik} x'_k$, is such that $\beta_{ns} = 0$, $\beta_{nn} \neq 0$, but otherwise $\beta_{nr} = \alpha_{nr}$. Hence we may multiply $\{\mathbf{T}\}$ by a product of central reflections such that finally $y_n = \gamma_{nn} x_n$. But for an *orthogonal* transformation‡ we must have $\gamma_{nn} = \pm 1$, and x_n must disappear from the other equations, and therefore the proposition is established.

Referring to the preceding theorems we may now state the fundamental result.

THEOREM 7. *Every linear transformation of a general quadratic form in n variables into itself may be compounded of n central reflections or fewer, and theorems 1–5 hold for all such transformations.*

* For this interpretation of the variables, a central reflection becomes the usual reflection in a line through the origin.

† This theorem is given by KRONECKER, Berliner Monatsberichte (1890), p. 1071, whose proof is essentially identical with the following.

‡ Since $\sum_i \alpha_{is}\alpha_{in} = 0$ $(i, s = 1, 2, \cdots, n-1)$, and also $|\alpha_{in}| \neq 0$, we must have $\alpha_{in} = 0$, and from $\sum_i \alpha_{in}^2 + \gamma_{nn}^2 = 1$, $\gamma_{nn} = \pm 1$.

As already remarked, VOSS has proved that the *general* orthogonal substitution is compounded of n central reflections, and for this purpose he chooses the equations of the transformation in CAYLEY's form. He also points out that the determination of the centers is exactly analogous to that of finding a self-conjugate tetrahedron with respect to a quadric.* The association of the general transformation with a characteristic duality is implied in this statement, but very imperfectly. Moreover, since the formulas of CAYLEY apply only to *general proper* transformations, it is evident that the proof given by VOSS is incomplete.

§ 3. *Equations of the transformations† compounded of n independent central reflections.*

Since the general transformation is completely characterized by a correlation in which coincidence of point and corresponding M_{n-2} arises when the point is on the absolute, we begin with the duality $\{\Gamma\}$ defined by

$$\sum_{i,k} \beta_{ik} x_i y_k = 0 \qquad (i, k = 1, 2, \cdots, n). \tag{5}$$

For $x = y$, this must reduce to (1), or, $f(x) = 0$; i. e., $\beta_{ik} + \beta_{ki} = 2\lambda a_{ik}$. Then if we set $\beta_{ik} - \beta_{ki} = 2\mu\alpha_{ik}$, we may write $\{\Gamma\}$ in the form

$$\sum_{i,k} (\lambda a_{ik} + \mu\alpha_{ik}) x_i y_k = 0 \qquad (a_{ik} = a_{ki},\ \alpha_{ik} = -\alpha_{ki}). \tag{6}$$

The equation (6) gives the most general form of the correlation in question, and shows that for a given $f(x)$, the variety is given by the number of the arbitrary α's, viz., $\frac{1}{2}n(n-1)$; and accordingly, the number of essential parameters in the most general Hermite transformation is $\frac{1}{2}n(n-1)$.

The duality

$$f(x, y) \equiv \sum a_{ik} x_i y_k = 0 \tag{7}$$

is evidently the polar reciprocation with respect to the absolute, while

$$w(x, y) \equiv \sum \alpha_{ik} x_i y_k = 0 \qquad (\alpha_{ik} = -\alpha_{ki}) \tag{8}$$

is a *nullsystem*, since point and corresponding M_{n-2} lie in coincidence. The geometrical relation of the dualities (6), (7) and (8) is simply this. Under $\{\Gamma\}$ the point x gives the two M_{n-2}'s, M and M' say, whose equations are $\lambda f(x, y) + \mu w(x, y) = 0$, $\lambda f(x, y) - \mu w(x, y) = 0$; and therefore M and M' are divided harmonically by the polar of x with respect to the absolute and the correspondent of x in the nullsystem. ‡

* Loc. cit., p. 349.

† It will be convenient to designate any linear transformation of a quadratic form into itself, an *Hermite transformation*. (Cf. LOEWY, loc. cit.)

‡ Cf. *Vorlesungen über Geometrie*, CLEBSCH-LINDEMANN, vol. 2, p. 402, for the corresponding discussion in ordinary space.

We proceed now to find the equations of the Hermite transformation $\{\mathbf{T}\}$ corresponding to the correlation $\{\Gamma\}$ defined by (6).

Let $x\{\mathbf{T}\}x'$, and suppose $\{\mathbf{T}\} \equiv \{\mathbf{a}^{(1)}\mathbf{a}^{(2)}\cdots\mathbf{a}^{(n)}\}$, according to theorem 7. Choose a such that $a\{\Gamma\}M$, when M is the polar of x', i. e.,

$$\sum_i(\lambda a_{ik}+\mu\alpha_{ik})a_i \equiv \rho\sum_i a_{ik}x'_i \qquad (i,k=1,2,\cdots,n). \tag{9}$$

Then x' is an *invariant* point for $\{a\mathbf{T}\}$, and hence $x\{\mathbf{a}\}x'$. That is, we have to eliminate the a from (9) and

$$x = x' - \frac{2f(x',a)}{f(a)}a. \tag{10}$$

Multiplying (9) by a_k and summing with respect to k, gives $\lambda f(a) = \rho f(x', a)$; hence (10) becomes

$$x = x' - \frac{2\lambda}{\rho}a; \tag{11}$$

and now eliminating a from (9) and (11) we obtain

$$\sum_i(\lambda a_{ik}-\mu\alpha_{ik})x'_i + \sum_s(\lambda a_{sk}+\mu\alpha_{sk})x_s = 0 \qquad (i,k,s=1,2,\cdots,n). \tag{12}$$

The equations† of $\{\mathbf{T}\}$ are then found by solving (12) for x'. Before taking up this question, however, an interesting geometrical theorem is at once read out of (12), viz.,

THEOREM 8. *Corresponding points in any general Hermite transformation are points which give the same M_{n-2} in the duality which is characteristic of the transformation.*

This theorem completes the connection between the transformation $\{\mathbf{T}\}$ and its corresponding duality, and would serve as basis of a purely geometrical discussion.

The equations of $\{\mathbf{T}\}$ in the form† (12) are very convenient for discussion as the following deductions will show.

Write (12) when solved for x' in the form

$$x'_i = \sum_k c_{ik}x_k \qquad (i,k=1,2,\cdots,n). \tag{13}$$

Then denoting the determinant $|\lambda a_{ik}+\mu\alpha_{ik}|$ by $\Delta(\lambda,\mu)$, we evidently have

$$|c_{ik}| \equiv (-1)^n\frac{\Delta(\lambda,\mu)}{\Delta(\lambda,-\mu)} = (-1)^n, \tag{14}$$

for $\Delta(\lambda,-\mu)$ is simply $\Delta(\lambda,\mu)$ with rows and columns interchanged. This

* Multiplying (12) by x'_k and x_k, respectively, and summing with respect to k gives $f(x)=f(x')$, a verification.

† I do not find the Hermite transformation so given elsewhere. See, for example, LOEWY, loc. cit., pp. 9 et seq.

result is a verification, for the determinant of a central reflection is -1, and of course of $\{\mathbf{T}\}$, should be $(-1)^n$. Hence

THEOREM 9. *The equations* (12) *define a proper or improper Hermite transformation according as n is even or odd.*

The solution of (12) is obtained at once by first solving (9) for the a's and then substituting in (11). Following this method we readily find for the c's of (13) the equations:

$$(15)\qquad c_{ii} = \frac{\Delta(\lambda,\mu) - 2\lambda\sum_k a_{ki}\Delta_{ki}(\lambda,\mu)}{\Delta(\lambda,\mu)}, \qquad c_{is} = \frac{-2\lambda\sum_k a_{ks}\Delta_{ki}(\lambda,\mu)}{\Delta(\lambda,\mu)}$$
$$(i \neq s;\ i, k, s = 1, 2, \cdots, n).$$

The classical formulas of Cayley for an orthogonal substitution are of course obtained by setting $a_{ik} = 0$, $i \neq k$, $a_{ii} = 1$.

Associated with the same nullsystem α_{ik} are ∞^1 dualities determined by the ratio $\lambda : \mu$. An interesting result is obtained by putting $\mu = 0$: for then the duality becomes the polar reciprocation in the absolute. The centers of $\{\mathbf{T}\}$ are now conjugate in pairs and therefore reflections in these centers are commutative (§ 1). The equations (12) become simply $x_i' = -x_i$, and we get

THEOREM 10. *The transformation in R_{n-1} compounded of n commutative central reflections in the absolute reduces to an identical point transformation.*

This result is obtained by VOSS (loc. cit., p. 345), who also gives interesting geometrical consequences for $n = 3$ and $n = 4$. Compounding $\{\mathbf{T}\}$ with $x_i' = -x_i$ gives a *proper* transformation for every n. If n is odd, however, the product reduces down to one of $n-1$ central reflections. In this case, therefore, the transformation compounded of n and of $n-1$ central reflections are essentially identical.

The unsolved form (12) of $\{\mathbf{T}\}$ is* very convenient for discussion of fixed elements. For, putting $x' = \rho x$, we find

$$(15a)\qquad \phi(\rho) \equiv |\lambda a_{ik}(\rho+1) - \mu\alpha_{ik}(\rho-1)| = 0,$$

the corresponding fixed point x being given by

$$\sum_i [\lambda\alpha_{ik}(\rho+1) - \mu\alpha_{ik}(\rho-1)]\, x_i = 0.$$

Evidently $\phi(1) \neq 0$ if $|a_{ik}| \neq 0$, and we learn that *the characteristic equation*† *of the transformation* (15) *cannot have the root* $+1$ *if the absolute is non-degenerate.*

Geometrically, the determination of the fixed elements is the same as the

*Cf., e. g., LINDEMANN, Münchener Berichte (1896), p. 52.

†The "characteristic function" of (13), (15) is readily seen to be $\phi(\rho) \div (-1)^n\Delta(\lambda,\mu)$, since for $\rho = 0$, the characteristic function must reduce to $|c_{ik}|$ or $(-1)^n$.

question of coincident elements in the polar reciprocation (7) and the nullsystem (8).

§ 4. *The transformations compounded of n central reflections or fewer.*

The transformation $\{\mathbf{T}_{n-t}\} \equiv \{\mathbf{a}^{(1)}\mathbf{a}^{(2)}\cdots\mathbf{a}^{(n-t)}\}$, $t>0$, becomes a $\{\mathbf{T}_n\}$ if multiplied by any $\{\mathbf{T}_t\}$ whose locus of centers does not intersect the locus of centers of $\{\mathbf{T}_{n-t}\}$. The correlation *within* the latter M_{n-t-1} which is characteristic of $\{\mathbf{T}_{n-t}\}$ is therefore determined by a duality (6), in the sense that a point in M_{n-t-1} corresponds to the M_{n-t-2} determined by the intersection of M_{n-t-1} and the M_{n-2} corresponding to the point by (6). Furthermore, it is evident that the relation

$$\{\mathbf{T}_n\} \equiv \{\mathbf{T}_t\mathbf{T}_{n-t}\}$$

indicated above, implies that the locus of centers of $\{\mathbf{T}_t\}$ corresponds under the duality defining $\{\mathbf{T}_n\}$ to the locus of centers M_{n-t-1} of $\{\mathbf{T}_{n-t}\}$. As remarked before, these must not intersect. The necessary and sufficient condition is found. For if M_{n-t-1} is defined by

$$(\nu^{(1)}x)=0,\ (\nu^{(2)}x)=0,\ \cdots,\ (\nu^{(t)}x)=0, \tag{16}$$

then the corresponding M_{t-1} under (6) is determined from

$$\sum_i(\lambda a_{ik}+\mu\alpha_{ik})a_i=\sigma^{(1)}\nu_k^{(1)}+\sigma^{(2)}\nu_k^{(2)}+\cdots+\sigma^{(t)}\nu_k^{(t)}\quad(i,k=1,2,\cdots,n). \tag{17}$$

If then the a's satisfy (16), the condition appears in the vanishing of the determinant formed by bordering $\Delta(\lambda,\mu)$ by the ν's. Denoting this bordered determinant by

$$\Delta^{(t)}(\lambda,\mu),$$

we have

THEOREM 11. *The necessary and sufficient condition for the intersection of an M_{n-t-1} (16) with the M_{t-1} corresponding to it under any duality is found by equating to zero the determinant of order $n+t$ formed by bordering the determinant of the duality with the ν's.*

In particular, $\Delta^{(1)}(\lambda,\mu)=0$ defines in the coördinates v_i the correlate of the absolute itself under $\{\Gamma\}$. That is, the envelope of the M_{n-2}'s which contain their corresponding points. This quadratic manifold is the second "fundamental locus" of the duality, the other being the absolute itself.*

Proceeding now to find the equations of $\{\mathbf{T}_{n-t}\}$, the locus of centers being defined by (16) and $\Delta^{(t)}(\lambda,\mu)\neq 0$, we may at once write down the equations of the most general duality within M_{n-t-1} such that the M_{n-t-2} determined by any point shall lie in the M_{n-2} corresponding to that point under (6). These are

* LINDEMANN, *Vorlesungen* etc., vol. 2, p. 402; Voss, Mathematische Annalen, vol. 13 (1878), p. 359.

$$(18)\quad \sum_i(\lambda a_{ik}+\mu\alpha_{ik})a_i+\sigma^{(1)}\nu_k^{(1)}+\sigma^{(2)}\nu_k^{(2)}+\cdots+\sigma^{(t)}\nu_k^{(t)}=\rho u_k \quad (i,k=1,2,\cdots,n).$$

The a's satisfy (16) also, or

$$(19)\qquad (\nu^{(1)}a)=0,\ (\nu^{(2)}a)=0,\ \cdots,\ (\nu^{(t)}a)=0.$$

The $n+t$ equations (18) and (19) may be solved for the a's and σ's, since $\Delta'(\lambda,\mu)\neq 0$. The a's depend only upon the *intersection* of $(ux)=0$ and the M_{n-t-1} (16).

As before, if $x\{\mathbf{T}_{n-t}\}x'$, then choosing for u the polar M_{n-2} of x' with respect to $f=0$, i. e., taking in (18),

$$(20)\qquad u_k=\sum_i a_{ik}x_i',$$

and assuming the a determined by (18) as the *first* center of $\{\mathbf{T}_{n-t}\}$, then obviously $x\{\mathbf{a}\}x'$, as in the general case, § 3. Multiplying (18) by a_k and summing with respect to k, gives by (19) and (20) $\lambda f'(a)=\rho f'(x',a)$. Hence the equations of the a's are

$$(21)\qquad x_i-x_i'+\frac{2\lambda}{\rho}a_i=0.$$

The equations of $\{\mathbf{T}_{n-t}\}$ are then found by the elimination of the a's, the u's, and the σ's from (18), (19), (20), and (21). In fact substituting from (20) and (21) in (18) and (19), gives

$$(22)\qquad \sum_i(\lambda a_{ik}+\mu\alpha_{ik})x_i+\sum_j(\lambda a_{jk}-\mu\alpha_{jk})x_j'-\frac{2\lambda}{\rho}\sum_s\sigma^{(s)}\nu_k^{(s)}=0$$
$$(i,j,k=1,2,\cdots,n;\ s=1,2,\cdots,t),$$

$$(23)\qquad (\nu^{(s)}x)-(\nu^{(s)}x')=0.$$

Multiplying (22) by x_k and x_k' respectively and summing with respect to k gives as before the verification

$$f(x)=f(x').$$

We may therefore state

THEOREM 12. *The equations* (22) *and* (23) *define in unsolved form a linear transformation of the quadratic form $f(x)$ into itself, and every such transfortion is given by these equations, t having any value from* 0 *to* $n-1$, *and the α's being elements of an arbitrary skew determinant.*

The form $x_i'=\sum c_{is}x_s$ for the transformation is readily obtained by solving (18), (19), (20) for a_i and substituting in (21). This gives

$$(24)\qquad c_{is}=e_{is}-\frac{2\lambda\sum_k a_{ks}\Delta_{ki}^{(t)}(\lambda,\mu)}{\Delta^{(t)}(\lambda,\mu)},$$

where

$$e_{is}=0\,(i\neq s),\ e_{ii}=1 \qquad (i,k,s=1,2,\cdots,n).$$

THEOREM 13. *The equations* (24) *give the form of the coefficient of every Hermite transformation.*

The determinant $|c_{is}| = (-1)^{n-t}$. This is easily seen by making a change of variable $y_s = (\nu^{(s)}x)$, $s = 1, 2, \cdots, t$, by which $n-t$ of the x's remain unchanged, say $x_{t+1}, \cdots, x_n$, it being assumed that the determinant

$$|\nu_1^{(1)}\nu_2^{(2)}\cdots\nu_t^{(t)}| \tag{25}$$

of the matrix

$$||\nu_1^{(1)}\nu_2^{(1)}\cdots\nu_t^{(1)}|| \tag{26}$$

does not vanish.

This transformation may readily be effected by first eliminating the σ's, and then changing the variables.

The α's are still arbitrary in (24), but no longer essential. In fact, (18) and (19) defining a duality in a linear M_{n-t-1}, contain at most $\frac{1}{2}(n-t)(n-t-1)$ essential parameters. And indeed, if the σ's and $a_1, a_2, \cdots, a_t$ be eliminated from (18) and (19) under the hypothesis (25) made above, there will remain $(n-t)$ equations for $a_{t+1}, \cdots, a_n$, of the form

$$\sum_j (\lambda a'_{t+j,\,t+k} + \mu\alpha'_{t+j,\,t+k})a_{t+j} = \rho u'_{t+k} \qquad (j, k = 1, 2, \cdots, n-t), \tag{27}$$

in which the a''s and α''s are linear in the a's and α's respectively, and at the same time elements of a symmetric and skew determinant respectively. The coefficients of the a's and α's are quadratic in the determinants of order t of the matrix (25).

Since the number of independent determinants is $t(n-t)$, we find for the total number of essential parameters in (24),

$$\tfrac{1}{2}(n-t)(n-t-1) + t(n-t) = \tfrac{1}{2}(n-t)(n+t-1),^*$$

which agrees with the statement of Theorem 5 for $r = n-t$.

Returning to (22) and (23) for discussion of fixed elements $x' = \rho x$, we find for the characteristic function of (24),

$$\phi(\rho) = \frac{(-1)^{n-t}(\tilde{1}-\rho)^t\phi^{(t)}(\rho)}{\Delta^{(t)}(\lambda, \mu)}, \tag{28}$$

where $\phi^{(t)}(\rho)$ is the determinant (15a) of the general case bordered with the ν's. It is easy to transform $\phi^{(t)}(\rho)$ into the determinant of order $n-t$,

$$\phi^{(t)}(\rho) = |\lambda a'_{t+j,\,t+k}(\rho+1) - \mu\alpha'_{t+j,\,t+k}(\rho-1)|, \tag{29}$$

in which a' and α' have the same significance as above. The equations (28) and (29) give the theorem due to Voss.†

* Cf. LINDEMANN, Münchener Berichte (1896), p. 66.

† VOSS, Münchener Berichte (1896), p. 14.

The characteristic function for any Hermite transformation (24), *except for the factor* $(1-\rho)^t$, *always has the form*

$$|\lambda a'_{ik}(\rho+1)-\mu\alpha'_{ik}(\rho-1)| \qquad (i,k=1,2,\cdots,n-t),$$

in which the a'*s and* α'*s are elements of a symmetric and skew determinant respectively.*

Finally, (22) and (23) show that $\rho=1$ gives for the corresponding fixed point

$$\rho\sum_i \lambda a_{ik}x_i=\sum_s \sigma^{(s)}v_k^{(s)},$$

i, e., *every* point of the polar of the M_{n-t-1} (16) with respect to the absolute is fixed. Any other fixed point lies in the M_{n-t-1} (16), the discussion of their arrangement being precisely that of the general case if n is replaced by $n-t$.

The problem of the determination of all linear transformations of a quadratic form into itself may therefore be regarded as completely solved in this and the preceding sections. The derivation of canonical forms for any given case is a matter of no great difficulty. The question evidently depends primarily upon the discussion of the dualities (7) and (8) of § 3.

§ 5. *Further resolution of the transformation into involutory transformations.*

The inverse $\{\mathbf{T}_{n-t}^{-1}\}$ of the transformation (22), (23) is found by changing μ to $-\mu$. Hence $\{\mathbf{T}_{n-t}\}$ is involutory when and only when $\mu=0$, i. e., when $\{\mathbf{T}_{n-t}\}$ is compounded of reflections in centers conjugate with respect to the absolute. Such a transformation depends upon $t(n-t)$ essential parameters, viz., the coördinates of the locus of centers.

We now state the theorem:

THEOREM 14. *Every linear transformation of a quadratic form into itself may be resolved into the product of two involutory transformations.*

Consider any $\{\mathbf{T}_t\}$, $t=2r$; then we shall prove

$$\{\mathbf{T}_t\}\equiv\{\mathbf{a}_1,\mathbf{a}_2,\cdots,\mathbf{a}_r\}\{\mathbf{b}_1,\mathbf{b}_2,\cdots,\mathbf{b}_r\}, \tag{30}$$

where the a's and also the b's are conjugate in pairs.

For simplicity of statement, take $r=2$. Then the locus of centers of $\{\mathbf{T}_4\}$ is ordinary space, M_3, the transformation being characterized by a duality $\{\mathbf{\Gamma}\}$ in M_3, which is pointed out in § 3, is defined by means of a nullsystem $\{\mathbf{N}\}$ together with reciprocation in the absolute. From (6) and (8) § 3, it is readily seen that $\{\mathbf{a}_1\mathbf{a}_2\}\equiv\{\mathbf{a}_2\mathbf{a}_1\}$ when and only when a_2 lies in the plane corresponding to a_1 under $\{\mathbf{N}\}$. Thus the line A joining a_1, a_2 is invariant under $\{\mathbf{N}\}$, that is, A "belongs to $\{\mathbf{N}\}$," and the line B determined by b_1, b_2 enjoys the

same property.* Furthermore $A\{\Gamma\}B$, by theorem 5. Hence, since the ∞^3 lines of $\{\mathbf{N}\}$ transform by $\{\Gamma\}$ into the ∞^3 lines of a nullsystem $\{\mathbf{N}'\}$, it appears that the line A of $\{\mathbf{N}\}$ becomes B of $\{\mathbf{N}'\}$, that is, B belongs to $\{\mathbf{N}\}$ and $\{\mathbf{N}'\}$. Through any point b_1 passes one line of the congruence common to $\{\mathbf{N}\}$ and $\{\mathbf{N}'\}$, hence if b_1 is chosen arbitrarily, B is determined uniquely, and also A from $A\{\Gamma\}B$, but a_1 is any point on A. Thus the resolution may be effected in ∞^2 ways.

The proof for $r > 2$ is precisely the same, and the degree of freedom is found to be r. For $t = 2r - 1$, it is only necessary to multiply $\{\mathbf{T}_t\}$ by an $\{\mathbf{a}\}$, and then apply the theorem, remembering that a may be chosen arbitrarily. For $n = 2r - 1$, it has already been remarked that the transformation is not different from $t = 2r - 2$.

As a general theorem, it may be stated that the resolution†

$$\{\mathbf{T}_t\} \equiv \{\mathbf{T}_\lambda \mathbf{T}_\mu \mathbf{T}_\nu \cdots\}$$

into involutory transformations may be effected in

$$\tfrac{1}{2}t(t+1) - (\lambda^2 + \mu^2 + \nu^2 + \cdots)$$

ways.

§6. *Application to the case* $n = 6$.

Special interest attaches to the case $n = 6$, for then the x's satisfying $f(x) = 0$, $|a_{ik}| \neq 0$, may be assumed as line coördinates in ordinary space, R_3, central reflection becomes the transformation defined by a nullsystem in R_3, or, inversion in a linear line complex, while the transformations $\{\mathbf{T}_t\}$ in question are the collineations and correlations of projective geometry, according as t is even or odd. In other words, we are concerned with line geometry in the sense of PLÜCKER. The involutory transformations $\{\mathbf{T}_2\}$ and $\{\mathbf{T}_3\}$ are respectively a skew reflection‡ and polar reciprocation in a quadric. Theorem 14 now gives the well known results that a general collineation is compounded of two polar reciprocations, and the general correlation of a skew reflection and a polar reciprocation. Resolving

$$\{\mathbf{T}_6\} \equiv \{\mathbf{T}_2\}\{\mathbf{T}_2'\}\{\mathbf{T}_2''\}, \tag{31}$$

gives the theorem due to WILSON, that the general collineation is compounded of three skew reflections. The resolution possesses nine degrees of freedom, and the discussion brings out some essential facts not given in the theorem of WILSON.

Let $\{\mathbf{T}_2\}$ in (31) be $\{\mathbf{ab}\}$. Then if x and x' are the directrices of $\{\mathbf{T}_2\}$,

* For discussion of the nullsystem of MÖBIUS, reference may be made to LINDEMANN, *Vorlesungen*, vol. 2, p. 52.

† Voss has given theorem 14 for $t = n = 2r$; Mathematische Annalen, vol. 13, p. 343.

‡ Cf. WILSON, Transactions, vol. 1 (1900), pp. 193–196.

$a = x + \lambda x'$, $b = x - \lambda x'$, and from the duality $\lambda f'(x, y) + \mu w(x, y) = 0$ defining $\{\mathbf{T}_6\}$, since a and b satisfy this, and also $f(a, b) = 0$, we find

$$\sum \alpha_{ik} x_i x'_k = 0 \qquad (a_{ik} = -a_{ki}), \tag{32}$$

and the directrices of each component of $\{\mathbf{T}_6\}$ satisfy (32). Furthermore, it is readily found that the directrices of $\{\mathbf{T}'_2\}$ and $\{\mathbf{T}''_2\}$ belong to the congruence common to the complexes,

$$\lambda f(x, y) + \mu w(x, y) = 0, \qquad \lambda f(x', y) + \mu w(x', y) = 0, \tag{33}$$

and one line of this congruence may be chosen arbitrarily. The complete result therefore is

THEOREM 15. *A general collineation may be resolved in ∞^9 ways into the product of three skew reflections. The first pair of directrices satisfy* (32) *in three-dimensional space. Either one having been chosen, the other belongs to a linear line complex containing the first. The remaining four directrices then belong to the linear line congruence* (33), *and one having been chosen arbitrarily the other three are determined uniquely.*

§ 7. *Linear transformation of the alternating bilinear form into itself.*

The alternating form

$$w(x, y) \equiv \sum \alpha_{ik} x_i y_k = 0 \qquad (a_{ik} = -a_{ki}), \tag{34}$$

is invariant under the transformation obtained from (22) and (23) by changing the sign of the x' in (22); viz.,

$$\sum_k (\lambda a_{ik} + \mu \alpha_{ik}) x_i - \sum_i (\lambda a_{ik} - \mu \alpha_{ik}) x'_i - \frac{2\lambda}{\rho} \sum_s \sigma^{(s)} \gamma_k^{(s)} = 0, \tag{35}$$

$$(v^{(s)} x) - (v^{(s)} x') = 0 \qquad (s = 1, 2, \cdots, t), \tag{36}$$

$$a_{ik} = a_{ki} \qquad (i, k = 1, 2, \cdots, n),$$

x and y being cogredient variables. For multiplying (35) by y_k and summing up, with respect to k,

$$\lambda f(x, y) + \mu w(x, y) - \lambda f(x', y) + \mu w(x', y) - \frac{2\lambda}{\rho} \sum \sigma^{(s)} (v^{(s)} y) = 0. \tag{37}$$

In the same way are found three other equations, and from these is found by using (36),

$$w(x, y) = w(x', y').$$

The determinant of the solution of (35), (36) is $+1$, the reasoning being the same as in § 4. The characteristic function is therefore

$$\phi(\rho) = \frac{(1-\rho)^t \phi^t(-\rho)}{\Delta^{(t)}(\lambda, \mu)},$$

$\phi^{(t)}(\rho)$ having same meaning as in (28).

The a's in (35) are arbitrary, but not essential parameters. The number of the latter is readily found to be

$$\tfrac{1}{2}(n-t)(n-t+1) + t(n-t) = \tfrac{1}{2}(n-t)(n+t+1).$$

By the method of this section all linear transformations of the required type are found.*

*Cf. Voss, Münchener Berichte (1896), p. 20.

THE SHEFFIELD SCIENTIFIC SCHOOL,
YALE UNIVERSITY.

A SET OF POSTULATES FOR REAL ALGEBRA, COMPRISING POSTULATES FOR A ONE-DIMENSIONAL CONTINUUM AND FOR THE THEORY OF GROUPS*

BY

EDWARD V. HUNTINGTON

CONTENTS.

PAGE.

§ 1. A set of postulates for a one-dimensional continuum..... 18
§ 2. A set of postulates for abelian groups..... 22
§ 3. A set of postulates for real algebra..... 24
§ 4. Summary of the postulates, and proofs of their independence..... 31

§ 5. Further analysis of the postulates for group-theory..... 34
§ 6. Another set of postulates for real algebra..... 36
§ 7. A condensed list of postulates..... 38
Appendix.† A set of postulates for realalg ebra, in which multiplication is included as a fundamental concept..... 39

The postulates for real algebra presented in this paper may be analysed into three groups: (1) propositions concerning the relation $<$, which, taken by themselves, form a set of independent postulates for a one-dimensional continuum, or a continuous scale; (2) propositions concerning the operation $+$, which, taken by themselves, form a set of independent postulates for the theory of groups; and (3) propositions connecting the two symbols $<$ and $+$. All these postulates taken together form a complete set of postulates for real‡ algebra as given in §§ 1–4. Various modifications of this set are given in the later sections of the paper and in the appendix.

All these postulates are shown to be *independent*, that is, the list contains no redundancies; and the system which they determine is shown to be unique, §

* Presented to the Society at the St. Louis summer meeting, September 17, 1904, and to the Congress of Arts and Sciences, Section of Algebra and Analysis, St. Louis, September 22, 1904. Received for publication September 17, 1904.

† Received for publication October 3, 1904.

‡ A set of postulates for *complex* algebra will be presented in a subsequent paper.

§ A set of postulates having this property has been called a "categorical," as distinguished from a "disjunctive," set; see O. VEBLEN, Transactions, vol. 5 (1904), p. 346. Every proposition concerning a class K, a relation $<$, and an operation $+$, is either deducible from the postulates of this set, or in contradiction with them.

that is, there is essentially only one system (namely the system of all real numbers) in which a relation $<$ and an operation $+$ are so defined as to satisfy all the postulates (see below, theorem 30.) The existence of the system of real numbers, as built up from the positive integers by the "genetic" method of successive generalization of the number concept, * proves, moreover, the *consistency* of the postulates.

The postulates for a continuum (§ 1) are the obvious ones (see, for example, SCHÖNFLIESS's *Bericht über Mengenlehre*†), but their independence has not heretofore been established.

The postulates for the theory of groups (§ 2 and § 5) carry the analysis farther, it is thought, than the earlier sets given by the writer‡ and by E. H. MOORE.§

The postulates for real algebra (§ 3 and § 6) are more satisfactory than the writer's earlier set‖ in several respects; first, the separation of the postulates concerning $<$ from those concerning $+$ is now complete; secondly, the individual postulates are more nearly simple statements (and are hence more numerous); and finally, in the statement of the postulates no assumption is made in regard to the existence of any kind of numbers. This last improvement was suggested by a recent paper by BURALI-FORTI, to which further reference will be made in § 3.

On the fundamental concepts involved, namely: *class*, and *element* of a class; *dyadic relation*; and *operation*, or *rule of combination*; see Transactions, vol. 5 (1904), p. 288–290; for further bibliographical references see also Transactions, vol. 3 (1902), p. 265, and vol. 4 (1903), p. 358; and the *Theoretische Arithmetik* of STOLZ and GMEINER (1901 —).

§ 1. A SET OF POSTULATES FOR A ONE-DIMENSIONAL CONTINUUM.

In this section we consider the conditions which must be imposed upon a *class* K, and a *dyadic relation* $<$ (read: "below," or "algebraically less than"),¶ in order that K shall be a *one-dimensional continuum*, or a *continuous scale* with respect to $<$. These conditions are expressed in the following eight postulates: I, II, $R1$–$R6$ (the letter R being prefixed to indicate that the postulates concern the Relation $<$).**

* Cf. D. HILBERT, *Über den Zahlbegriff*, Jahresbericht der deutschen Mathematiker-Vereinigung, vol. 8 (1900), part 1, pp. 180–184.

† *Ibid.*, vol. 8 (1900), part 2.

‡ E. V. HUNTINGTON, Bulletin of the American Mathematical Society, ser. 2, vol. 8 (1901–2), pp. 296–300; Transactions, vol. 4 (1903), pp. 27–30.

§ E. H. MOORE, Transactions, vol. 3 (1902), pp. 485–492; vol. 5 (1904), p. 549.

‖ Transactions, vol. 4 (1903), pp. 358–370.

¶ Since the notion of *quantity* is not involved here, the expressions "below" and "above" (compare a thermometer scale) are clearly preferable to "less than" and "greater than." The expressions "before" and "after" may also be used to advantage.

** A summary of these postulates will be given in § 4.

The symbol $\prec$ here denotes a general dyadic relation, having no properties not expressly stated in the postulates. When, as in § 4, there is danger of confusion with the ordinary $<$ of arithmetic, we shall enclose the more general symbol in a circle, thus: $\circledcirc$; but the omission of the circle, whenever it is not absolutely necessary, will give the theorems a more familiar appearance, and thus facilitate the reading. Note that $a \prec b$ (a "below" b) and $b \succ a$ (b "above" a) denote the same relation between a and b; and that $a \preceq b$ means: $a \prec b$ or $a = b$.

POSTULATE I. There is an entity which belongs to the class.

This postulate tells us that K is not an "empty" class.

POSTULATE II. If a is an element of the class, there is an element b such that $a \neq b$.

This postulate excludes the trivial case of a class containing only a single element. — Postulates I and II together give us

Theorem 1. *There are at least two distinct elements in the class.*

POSTULATE $R1$. If a and b are elements of the class, and $a \neq b$, then either $a \prec b$ or $a \succ b$.

POSTULATE $R2$. If a and b are elements of the class, and $a \neq b$, then $a \prec b$ and $a \succ b$ cannot both be true.

That is, the relation $\prec$ is "non-symmetric" for every pair of distinct elements.

POSTULATE $R3$. If a is an element of the class, then $a \prec a$ cannot be true.

That is, the relation $\prec$ is "non-reflexive" for every element of the class. — From postulates $R1$–$R3$ we have at once:

Theorem 2. *If a and b are elements of the class, then either*

$$a = b, \qquad a \prec b, \qquad \text{or} \qquad a \succ b;$$

and these three relations are mutually exclusive.

POSTULATE $R4$. If a, b, c are elements of the class, and $a \neq c$, then from $a \prec b$ and $b \prec c$ follows $a \prec c$.

In view of postulate $R2$, this postulate gives us

Theorem 3. *From $a \prec b$ and $b \prec c$ follows $a \prec c$, whenever a, b and c belong to the class.*

That is, the relation $\prec$ is "transitive."

The postulates $R1$–$R4$, with I and II, make the class a "scale" or a "simply ordered assemblage" with respect to the relation $\prec$; or, an assemblage possessing "*Grössencharakter*" in the sense defined by SCHÖNFLIESS (loc. cit.).

POSTULATE $R5$. If a and b are elements of the class such that $a \prec b$ or $a \succ b$, then: if $a \neq b$, there is either an element x such that $a \prec x$ and $x \prec b$, or an element y such that $a \succ y$ and $y \succ b$.

Such an element x (or y) is said to lie "between" the elements a and b; in view of theorems 1–3, we have

Theorem 4. *If a and b are two distinct elements, there is at least one, and therefore an infinite number of elements lying "between" them; and hence the class K itself is infinite.*

Thus postulate $R5$, taken with the preceding postulates, makes the class "dense" (*dicht, compact*) with respect to the relation $\prec$. (Without this postulate, the class might be infinite but "discrete," like the class of integral numbers, or, it might consist of merely a finite number of elements.) But a "dense" class is not necessarily continuous (as witness the system of all rational numbers with regard to $\prec$); we therefore add the following *postulate of continuity*, which may be stated in either of two forms, $R6$ or $R6'$:

POSTULATE $R6$. If Γ is a non-empty sub-class in K, and if there is an element c in K such that every element of Γ is $\prec c$, then there is an element X in K having the two following properties with regard to the sub-class Γ:

1°) if α is an element of Γ, then $\alpha \leqq X$; while

2°) if x is any element of K which is $\prec X$, there is an element in Γ which is $\succ x$.

This element X, which is readily seen to be uniquely determined by the sub-class Γ, is called the "upper limit" of the sub-class, or sometimes its "lowest upper bound." Thus, if a subclass Γ has *any* "upper bound" c in K, it will have a "*lowest* upper bound" X. If X happens to belong to the sub-class Γ, it is its highest element; but a sub-class Γ may have an upper limit and yet not have any highest element.

In place of postulate $R6$, and as equivalent to it, we might use

Postulate $R6'$: The same as postulate $R6$ with the symbols $\prec$ and $\succ$ interchanged.

In brief, if a sub-class Γ' has *any* "lower bound" in K, it will have a "*highest* lower bound," called also its "lower limit." This element will be uniquely determined by the sub-class Γ', and if it belongs to the sub-class it will be its lowest element.

Each of these postulates, $R6$ and $R6'$ can be deduced from the other (with the aid of the preceding postulates),* and from both together we have the following theorem:

Theorem 5. *If Γ and Γ' are two non-empty sub-classes in K, such that every element of Γ is $\prec$ every element of Γ', then there is at least one element M, which is $\leqq$ every element of Γ and $\leqq$ every element of Γ'.*

* Thus, suppose, in the first place, that $R6$ is given, then the proof for $R6'$ is as follows: In the hypothesis, the sub-class Γ' is a non-empty class, which has *some* lower bound, say c'; we are to prove that it has *a highest* lower bound, X'. To show this, we define a sub-class Γ as the class of all those elements in K which are below every element in Γ'. This class Γ will be a non-empty class, since it contains the element c', and it will have some upper bound, since any element of the non-empty class Γ' will answer that purpose. Therefore, by postulate $R6$, the sub-class Γ will have an upper limit, X. It is then easy to show that this element X will be the required lower limit of the sub class Γ'. — In like manner, $R6$ could be deduced from $R6'$.

For, Γ will have its upper limit, X, and Γ' will have its lower limit, X', by postulates $R6$ and $R6'$, and $X \leqq X'$. Then take $M = X$, or X', or any element which may lie between X and X'.

In particular, if the two sub-classes Γ and Γ' make up, together, the whole class K, the upper limit of Γ will coincide with the lower limit of Γ', there will be only one element M, and this will be either the highest element in Γ or the lowest element in Γ'.*

Thus every system $(K, <)$ which satisfies postulates I, II, $R1$–$R6$ will have the property of continuity as defined by DEDEKIND in his *Stetigkeit und irrationale Zahlen*, and may be called a *one-dimensional continuum* or a *continuous scale*, with respect to the relation $<$. [See below, end of § 1.]

Moreover, these eight postulates I, II, $R1$–$R6$, as will be shown in § 4, are *independent* of each other; that is, no one of them can be deduced from the remaining seven.

In conclusion, we notice that a one-dimensional continuum, or continuous scale, as defined by postulates I, II, $R1$–$R6$, may be either limited or unlimited, in either direction. To complete the discussion of the present section, therefore, we add the two following postulates, although they will not be required in the remainder of this paper:

Postulate $R7$. If a is an element of the class, and if there is any element $b \neq a$, then there is an element x such that $x < a$;

Postulate $R8$. If a is an element of the class, and if there is any element $b \neq a$, then there is an element y such that $y > a$.

Hence, the class has neither a lowest nor a highest element, but is unlimited in both directions.

The ten postulates: I, II, $R1$–$R8$, form a set of independent postulates (see § 4), which define completely the properties of an *unlimited* continuous scale with respect to $<$. For, if C and C' are two systems $(K, <)$ which satisfy all these postulates, they clearly can be brought into one-to-one correspondence † in such a manner that if $a < b$ in C, then $a' < b'$ in C', where a' and b' are the elements which correspond to a and b respectively. Hence the set is "categorical," ‡ that is, every proposition concerning K and $<$ must either be deducible from the postulates of the set, or be in contradiction with them.

[It should be noticed that these postulates, in spite of the fact that they form a categorical set, are hardly sufficient to define a continuum in the ordinary *geometric* sense of the word. For example, the class of positive real numbers

* Notice also that postulate $R6$ can be deduced from theorem 5 (with the aid of the preceding postulates), by taking as Γ' the subclass of all the elements of K which are $>$ every element of Γ.

† And that in an infinite number of ways.

‡ O. VEBLEN: loc. cit.

between 0 and 3, omitting the numbers x for which $1 < x \leqq 2$, is a class which satisfies all the conditions but is not a geometric continuum in any ordinary sense. All we can say is that it is *equivalent* to a continuum *as far as our relation* $<$ *is concerned.**]

§ 2. A SET OF POSTULATES FOR ABELIAN GROUPS.†

In this section we consider the condition which must be imposed upon a *class* K, and an *operation* or *rule of combination* $+$ (read: "plus"), in order that K shall be an *abelian group* with respect to $+$. These conditions are expressed in the following eight postulates: I, II, $A1$–$A6$ (the letter A being prefixed to indicate that the postulates concern Abelian groups, or if one will, the operation of Addition).‡

The symbol $+$ here denotes a general operation, having no properties not expressly stated in the postulates. When, as in § 4, there is danger of confusion with the ordinary $+$ of arithmetic, we shall enclose the more general symbol in a circle, thus: $\oplus$.

POSTULATE I. There is an entity which belongs to the class.

POSTULATE II. If a is an element of the class, there is an element b such that $a \neq b$.

These postulates serve to exclude the cases of an "empty" class, and a class containing a single element. Together they give

Theorem 1. *There are at least two distinct elements in the class.*

POSTULATE $A1$. If a and b are elements of the class, then $a + b$ is an element of the class.

This postulate states the fundamental property of a *group*, the element $a + b$ being called, for our present purpose,§ the "sum" of the elements a and b.

POSTULATE $A2$. If a, b, $a + b$, and $b + a$ are elements of the class, then

$$a + b = b + a.$$

This is the "commutative law" for the operation $+$, and is the characteristic property of abelian groups as distinguished from groups in general.

* On G. CANTOR's definition of a continuum, which differs somewhat from DEDEKIND's definition, see B. RUSSELL, *Principles of Mathematics*, vol. 1 (1903), chap. 36.

† For a further analysis of the postulates for the theory of groups, see § 5.

‡ A summary of these postulates will be given in § 4.

§ If we interpreted the operation $\oplus$ as "multiplication," as one usually does in the general theory of abstract groups, we should call $a \oplus b$ the "product" of a and b. So below, instead of the "zero-element" (0), the "negative of a" $(-a)$, the operation of "subtraction" $(b - a)$, etc., we should speak of the "unit element" (1), the "reciprocal of a" (a^{-1}), the operation of "division" (b/a), etc. Again, if we were dealing with groups of transformations, we should call 1 the "identical transformation," or the "identity," and a^{-1} the "inverse of a." Compare § 5.

POSTULATE *A*3. If a, b, c, $a+b$, $b+c$, $(a+b)+c$, and $a+(b+c)$ are elements of the class, then

$$(a+b)+c=a+(b+c).$$

This is the "associative law" for the operation $+$. These three postulates give us

Theorem 6.* (*a*) *The operation* $+$ *is always possible within the class, and it obeys* (*b*) *the commutative law and* (*c*) *the associative law.*

POSTULATE *A*4. If a, x, y, $a+x$, and $a+y$ are elements of the class, then from $a+x=a+y$ follows $x=y$.

Hence, in view of this commutative law, we have

Theorem 7. *A change in either* a *or* b *alone produces a change in* $a+b$.

POSTULATE *A*5. If there is any element in the class, then there is an element 0 such that $0+0=0$.

It is easy to show that for any such element 0, and for every element a, $a+0=0+a=a$; and hence that the element 0 is uniquely determined.† Thus we have the theorem:

Theorem 8. (*a*) *There is a uniquely determined element* 0 *such that* $0+0=0$; (*b*) *for every element* a

$$a+0=a \qquad \text{and} \qquad 0+a=a;$$

and (*c*) *if* $a+x=a$ *or* $x+a=a$, *then* $x=0$.

This element 0 may be called, for our present purpose, the "zero-element" of the class, the properties in theorem 8 being the "additive" properties of zero. When, as in § 4, there is any danger of confusing this symbol with the ordinary 0 of arithmetic, we shall enclose it in a circle, or (which is typographically more convenient) denote the element in question by z (the initial letter of "zero"), or by i (the initial letter of "identity").‡

POSTULATE *A*6. If there is a uniquely determined element 0 such that $0+0=0$, then for every element a there is an element $\bar{a}$ such that $a+\bar{a}=0$.

In view of postulate *A*4, this element $\bar{a}$ is uniquely determined by a, and may be called the "negative of a." ‡

Further, if we take $x=\bar{a}+b$, we have

$$a+x=a+(\bar{a}+b)=(a+\bar{a})+b=0+b=b;$$

hence,

* The theorem-numbers 2-5 have been used in § 1.

† Thus, if $z+z=z$, we have $z+(a+z)=z+(z+a)=(z+z)+a=z+(a)$, whence, by postulate *A*4, $a+z=a$, and, by the commutative law, $z+a=a$. Hence, if z_1 and z_2 were two elements such that $z_1+z_1=z_1$ and $z_2+z_2=z_2$, then $a+z_1=a$ and $b+z_2=b$, for all values of a and b; whence, taking $a=z_2$ and $b=z_1$, we should have $z_2+z_1=z_2$ and $z_1+z_2=z_1$; or, $z_1=z_2$.

‡ Compare footnote under postulate *A*1.

Theorem 9. (*a*) *Every two elements, a and b, determine uniquely a third element x, denoted by* $b - a$, *such that*

$$a + (b - a) = b ;$$

(*b*) *in particular,*

$$a - a = 0 ;$$

and (*c*) *the element* $0 - a$ *is usually abbreviated into* $-a$, *so that*

$$a + (-a) = 0 .$$

The element $b - a$ is called the "difference" b minus a, and the operation of finding it, the "subtraction" of a from b.*

From theorems 1, and 6–9, we see that *every system* $(K, +)$ *which satisfies the eight postulates*, I, II, *A*1–*A*6, *is an abelian group with respect to* $+$, according to the usual definition.† These eight postulates, as will be shown in § 4, are *independent* of each other; that is, no one of them can be deduced from the other seven. The complete theory of abelian groups would contain all the propositions which follow from these eight postulates by logical deduction.

In conclusion, it should be noticed that the eight postulates of § 2 form a "disjunctive," not a "categorical," set;‡ for an abelian group may contain any finite number of elements, or be infinite; and even if the number of elements in two groups is the same, the groups are not necessarily isomorphic; hence there are many propositions concerning K and $+$ which are neither deducible from these postulates, nor in contradiction with them.

§ 3. A SET OF POSTULATES FOR REAL ALGEBRA.

In this section, which forms the main part of the present paper, we consider the conditions which must be imposed upon a *class* K, with a *dyadic relation* $\prec$ (read: "below," or "algebraically less than"), and an *operation* $+$ (read: "plus"), in order that K shall be the class of *all real variables* with respect to $\prec$ and $+$. (On the use of the symbols $\prec$ and $+$, or $\circledcirc$ and $\oplus$, see the opening paragraphs in § 1 and § 2.) These conditions are expressed in sixteen postulates, § which fall into four groups as follows:

POSTULATES I–II. (As in § 1 or § 2.)

These postulates give the class at least two distinct elements.

* Compare footnote under postulate *A*1.

† H. WEBER, *Algebra*, vol. 2. Cf. E. V. HUNTINGTON, and E. H. MOORE, loc. cit.; and also G. A. MILLER, *Report on the groups of an infinite order*, Bulletin of the American Mathematical Society, vol. 7 (1900–1), pp. 121–130.

‡ O. VEBLEN, loc. cit.

§ A summary of these postulates is given in § 4.

POSTULATES $R1$–$R6$. (As in § 1.)

These postulates, with I and II, make the class a *continuous scale*, or a *one-dimensional continuum*, with respect to the relation $\prec$.

POSTULATES $A1$–$A6$. (As in § 2.)

These postulates, with I and II, make the class an *abelian group* with respect to the operation $+$.

POSTULATE $RA1$. If there is a uniquely determined element 0 such that $0 + 0 = 0$; and if a, b, and $a + b$ are elements of the class; and if $a > 0$ and $b > 0$; then $a + b > a$.

POSTULATE $RA2$. If there is a uniquely determined element 0 such that $0 + 0 = 0$; and if a, b, and $a + b$ are elements of the class; and if $a < 0$ and $b < 0$; then $a + b < a$.

These last two postulates serve to connect the symbols $\prec$ and $+$. In view of postulates I, II, and $A1$–$A5$, they give us at once:

Theorem 10. *If a and b are both above* 0, *then $a + b$ is above either of them; and if a and b are both below* 0, *then $a + b$ is below either of them.*

These sixteen postulates: I–II, $R1 - R6$, $A1 - A6$, $RA1$ and $RA2$, are *independent*, as will be shown in §4, so that no one of them can be deduced from the remaining fifteen. On the other hand, these sixteen postulates, or the theorems 1–10 which follow from them,* are *sufficient to define completely the algebra of a real variable.* The remainder of this section will be devoted to the proof of this latter statement, the necessary preliminary theorems, besides the theorems 1–10, grouping themselves under the following heads: 1) positive and negative elements; 2) multiples, with remarks on BURALI-FORTI's definition of number; 3) ARCHIMEDES' principle; and 4) submultiples, with the theorem of infinite divisibility.

Positive and negative elements.

The following theorems 11–17 are proved without the use of postulate $R5$ (on density) or postulate $R6$ (on continuity).

Theorem 11. *If a and b are both > 0, then $a + b > 0$; and if a and b are both < 0, then $a + b < 0$.* (By 10 and 3.)

Theorem 12. *If $a > 0$, then $-a < 0$; and if $a < 0$, then $-a > 0$.* (By 11 and 9.)

Thus the class K is composed of three mutually exclusive, non-empty subclasses: 1) the element 0; 2) the elements above 0, called the *positive* elements; 3) the elements below 0, called the *negative* elements. (By I, II, 12 and 3.)

Theorem 13. *If $x > 0$, then $a + x > a$; if $x < 0$, then $a + x < a$.*

The first part is clearly true when $a = 0$, and (by 10) when $a > 0$; the proof for the remaining case, $a < 0$, is as follows: Suppose $a + x \leqq a$, while

* It should be noted that the sixteen postulates are clearly deducible from the theorems 1–10.

$x > 0$ and $a < 0$; then $a + x < 0$, by 3, and $-x < 0$, by 12; hence by 10, $(a + x) + (-x) < a + x$, or, by 6 and 9, $a < a + x$, which contradicts the supposition. The second part may be proved in a similar way.

Theorem 14. *If $a < b$ there is a positive element x such that $a + x = b$ and a negative element y such that $a = b + y$; and conversely, if $x > 0$ in $a + x = b$, or if $y < 0$ in $a = b + y$, then $a < b$.* (By 9 and 13.)

Theorem 15. *If $x < y$, then $a + x < a + y$, and conversely.*

For, by 14, take $w < 0$ so that $x = y + w$. Then, by 13,

$$(a + y) + w < (a + y),$$

whence $a + (y + w) < a + y$, or $a + x < a + y$. The converse is proved indirectly, as usual.

Theorem 16. *If $a < b$ and $x < y$, then $a + x < b + y$.*

For, $a + x < a + y$, and $a + y < b + y$, by 15 and the commutative law; hence the theorem, by 3.

Theorem 17. *There is no highest element, and no lowest element, in the class.* (By 13.)

If we admit also the postulate of density ($P5$), we have further:

Theorem 18. *There is no highest or lowest element in the sub-class of positive elements, or in the sub-class of negative elements.*

Multiples.

The theory of the multiples of an element a is closely connected with the theory of the (finite) ordinal numbers (or positive integers). In fact C. BURALI-FORTI, in a recent memoir,* has shown that the theory of multiples can be developed without presupposing any knowledge of these numbers, and that the class of numbers can then be defined by means of the theory of multiples. For the present purpose, however, it seems best to assume the ordinal numbers as known, especially in view of a valuable discussion of BURALI-FORTI's work by L. COUTURAT, in a memoir † which came into my hands while writing this paper.

In order to state precisely what is involved in thus assuming the ordinal numbers, it may be well to recall the following facts.

The class of ordinal numbers, however it may be defined, is a class N which possesses the following characteristic properties, due to PEANO:‡

* C. BURALI-FORTI, *Sulla teoria generale delle grandezze e dei numeri*, Atti della R. Accademia delle Scienze di Torino, vol. 39 (1903–4), pp. 256–272. On BURALI-FORTI's proof of the commutative law, see footnote below, in § 6.

† L. COUTURAT, *Les principes des mathématiques; V: L' idée de grandeur*, Revue de Métaphysique et de Morale, vol. 12 (1904), pp. 675–698.

‡ For a brief account of these postulates, with bibliographical references, see Bulletin of the American Mathematical Society, ser. 2, vol. 9 (1902–3), pp. 41–46. An extended discussion is found in B. RUSSELL's *Principles of Mathematics*, vol. 1 (1903), chap. 14. A revised list, in which the number of postulates is reduced to four, has been given by A. PADOA, *Théorie des nombres entiers absolus*, Revue de Mathématiques, vol. 8 (1902), p. 48.

1. The class N contains a peculiar element, called the "first" ordinal number, and denoted by 1.

2. Every element m of the class N determines uniquely another element of N called the number "next following" the number m, and denoted by m^+, or seq m. $(1^+ = 2;\ 2^+ = 3;$ etc.)

3. For any number m, m^+ is different from 1.

4. If $m^+ = n^+$, then $m = n$.

5. If S is any class such that: (a) the number 1 belongs to S, and (b) the number m^+ belongs to S whenever the number m belongs to S; then every element of N belongs to S.

This list of five postulates comprises as much of the theory of the ordinal numbers as we need to assume in the present paper.

On the basis of these fundamental propositions, the *sum*, $p + q$, of two numbers, p and q, is the number defined by the following recurrent formulæ:

$$p+1 = p^+,\ p+2 = (p+1)+1,\ p+3 = (p+2)+1, \cdots,$$
$$p+(k+1) = (p+k)+1;$$

whence, by mathematical induction, $p + q = q + p$.

Their *product*, pq, is defined by the following recurrent formulae:

$$1p = p,\ 2p = 1p + p,\ 3p = 2p + p, \cdots, (k+1)p = kp + p;$$

whence, by mathematical induction, $pq = qp$.

Finally, if $p \neq q$, then there is either a number $\lambda(= p - q)$ such that $p = q + \lambda$, or else a number $\mu(= q - p)$ such that $q = p + \mu$, and not both; in the first case we write $p > q$ (p "greater than" q), in the second case, $p < q$ (p "less than" q).

Making use of these properties of the ordinal numbers, we may now define the multiples of any element of our abstract class K. But we must be careful to notice that the symbols $+$ and $<$, as used between two ordinal numbers, have nothing to do with the general symbols $+$ and $\prec$ (or $\oplus$ and $\ominus$) as used between the elements of K.

We define the mth *multiple*, ma, *of any element* a, m being any ordinal number, by the following recurrent formulæ:

$$1a = a,\ 2a = 1a + a,\ 3a = 2a + a,\ \cdots,\ (k+1)a = ka + a.$$

Hence, if p and q denote ordinal numbers, and a an element of K, we have at once:

Theorem 19. 1°) $pa + qa = (p+q)a$;

2°) $q(pa) = p(qa) = (qp)a = (pq)a = pqa$.

This theorem depends only on postulates I, II, and $A1$; the following theorems

20–22, however, require all the postulates except $R5$ (on density) and $R6$ (on continuity):

Theorem 20. *If a is above 0, the successive multiples of a form an ascending series: $(m+1)a > ma$; if a is below 0, the successive multiples of a form a descending series: $(m+1)a < ma$; and if $a = 0$, every multiple of a is 0: $ma = 0$.*

In particular, if $a \neq 0$, $pa = qa$ when and only when $p = q$.

Theorem 21. *If $a < b$, then $ma < mb$, and conversely.*

For, if $a < b$, then $a = b + x$, where $x < 0$, by 14; hence $ma = mb + mx$, where $mx < 0$, by 20. Therefore $ma < mb$, by 14. Conversely, if $ma < mb$, then $a < b$, since $a \geqq b$ leads to contradictions.

Theorem 22. *If $ma = mb$, then $a = b$.* (From 21.)

The principle of Archimedes.

The following theorem requires all the postulates except the postulate of density ($R5$).

Theorem 23. *If a and b are both above 0, there are multiples of a which are above b; and if a and b are both below 0, there are multiples of a which are below b.* (Principle of ARCHIMEDES.)

The proof of the first part is as follows: Suppose every multiple of a were $\leqq b$; then, by the postulate of continuity ($R6$), the class of multiples of a would have an upper limit, X, having the following properties:

1°) $na \leqq X$, for every ordinal number n (in particular, $a < X$); and

2°) if $x < X$, there is some multiple of a, say $n'a$, which is $> x$.

By theorem 14, take $x < X$ so that $x + a = X$; then by 2°), $n'a > x$ for at least one value of n'. Hence, by theorem 15 and the commutative law, $n'a + a > x + a$, whence $(n'+1)a > X$, which contradicts 1°).

The second part is proved in a similar way.

Submultiples.

The following lemma requires all the postulates except $R6$ (on continuity); while the theorem 24 to which it leads, requires the whole list.

Lemma. If m is any ordinal number, then, if a is positive, there is a positive element x such that $mx < a$; and if a is negative, there is a negative element y such that $my > a$.

Proof. The lemma is clearly true when $m = 1$, by 18, and if it is true when $m = n$, it will be true when $m = n + 1$. For (considering the case $a > 0$), if $nx < a$, then there is a positive ξ such that $nx + \xi = a$, by 14, and a positive x' such that $x' < x$ and $x' < \xi$, by 18. Then $nx' < nx$ by 21, whence, $nx' + x' < nx + \xi$, by 16, or $(n+1)x' < a$. Therefore the lemma is true for every value of m.—Similarly for the case $a < 0$.

Theorem 24. *If m is any ordinal number, then every element a determines uniquely an element denoted by a/m, called the mth submultiple of a, such that*

$$m(a/m) = a.$$

In particular:

$$a/1 = a \qquad \text{and} \qquad 0/m = 0.$$

Proof. We notice in the first place, by 22, that this element a/m, if it exists at all, will be uniquely determined by a and m. To prove the existence of any such element (for a positive a), we define two subclasses: Γ, containing all the positive elements y for which $my < a$; and Γ', containing all the positive elements y' for which $a < my'$. Now Γ and Γ' are non-empty classes, by the lemma just proved, and 18; and every element in Γ is $<$ every element in Γ', by 21. Hence, by theorem 5, there is a positive element X such that: 1°) every element in $\Gamma \leqq X$, and 2°) $X \leqq$ every element in Γ'. This element X is the required element a/m. For if mX were $< a$, there would be an element y in Γ which is $> X$, in contradiction with 1°)*; and if mX were $> a$, there would be an element y' in Γ' which is $< X$, in contradiction with 2°).† Therefore $mx = a$. — The proof is similar for a negative a.

Theorem 25. *If p and q are ordinal numbers such that $p < q$, then if a is above 0, $a/p > a/q$, and if a is below 0, $a/p < a/q$.*

In other words, if $a \neq 0$, increasing the value of m brings the element a/m nearer to 0. In particular, if $a > 0$, $a > a/m > 0$, and if $a < 0$, $a < a/m < 0$; where $m > 1$. (Proof indirect, by 20, 21 and 24.)

Theorem 26. *If a and b are both above 0, there are submultiples of a which are below b; and if a and b are both below 0, there are submultiples of a which are above b.* (Proof indirect, by 23 and 24.)

Theorem 27. *If p and q denote ordinal numbers, and a an element of K, then $p(a/q) = (pa)/q$.* (By 24.)

Hence we may denote either member of this equation by pa/q.

Any element of the form pa/q, where p and q are ordinal numbers, is called a *rational fraction* of a. In particular, $p0/q = 0$.

Theorem 28. *If $m; p, q, p', q'$, are ordinal numbers, then:*

(*a*) $mpa/mq = pa/q$.

(*b*) $pa/q + p'a/q' = (q'p + qp')a/qq'$.

(*c*) $pa/q = p'a/q'$ when and only when $q'p = qp'$.

Theorem 29. *If a is above 0 [below 0], then $pa/q < p'a/q'$ when and only when $q'p < qp'$ [or $q'p > qp'$].* (Proof by 20, 21 and 24.)

* Take $\xi > 0$ so that $mX + \xi = a$, by 14, and $\eta > 0$ so that $m\eta < \xi$, by the lemma, and let $y = X + \eta$. Then $my = mX + m\eta < mX + \xi = a$.

† Take $\xi' < 0$ so that $mX + \xi' = a$, by 14, and $\eta' < 0$ so that $m\eta' > \xi'$, by the lemma, and let $y' = X + \eta'$. Then $my = mX + m\eta' > mX + \xi' = a$.

The theorems 1–29 put us now in a position to establish the fact that the postulates of § 3 are sufficient to define completely the algebra of a real variable; this sufficiency is formulated in the following theorem:

Theorem 30. *Any two systems,* $(K, <, +)$ *and* $(K', <, +)$, *which satisfy the sixteen postulates of* § 3 *are* EQUIVALENT *with respect to* $<$ *and* $+$; *that is, they can be brought into one-to-one correspondence* in such a way that*

1°) *from* $a < b$ *follows* $a' < b'$, *and conversely; and*

2°) *from* $a + b = c$ *follows* $a' + b' = c'$, *and conversely;*

where a', b', c' *are the elements in* K' *which correspond to the elements* a, b, c *in* K.

Proof. First make the zero-element in K correspond to the zero-element in K'.

Next, to bring the positive elements of K into one-to-one correspondence with the positive elements of K', choose any positive element E in K, and any positive element E' in K', and call E and E' corresponding elements; then if any positive element a is given, the corresponding positive element a' is determined as follows: consider in K the subclass Γ composed of all rational fractions of E which are $< a$; form in K' the subclass Γ' composed of the *same* rational fractions of E'; then the upper limit of Γ' is the required element a'. Similarly if a' is given and a required.

Finally, bring the negative element of K into one-to-one correspondence with the negative elements of K' by making a correspond to a' whenever $-a$ correspond to $-a'$.

The correspondence as thus established is readily shown to have the properties 1°) and 2°), by the aid of the theorems in regard to rational fractions.

Note on multiplication.

The deductions from the postulates have been carried, in this section, only so far as was necessary for the proof of theorem 30. The further development of the algebra depends on the definition of the *product* of two elements, with respect to an arbitrarily chosen (positive) "unit element."† [The arbitrary choice of this "unit element" is of great significance in the *theory of measurement*, into which I shall not enter here.]

Multiplication may also be regarded as a fundamental operation whose properties are determined by postulates, as is done below, in the appendix.

* And that in an infinite number of ways, since the "unit elements" E and E' in the proof may be chosen in an infinite number of ways.

† Cf. E. V. HUNTINGTON, Transactions of the American Mathematical Society, vol. 4 (1903), p. 365.

§ 4. Summary of the postulates, and proof of their independence.

In the following summary of the postulates of § 3 for real algebra, each postulate is stated twice, first in the precise and convenient symbolism * of Peano's *Logica Mathematica*, and secondly in common language. To avoid confusion in the proofs of independence, we enclose the general symbols $\prec$ and $+$ in circles, and write z in place of 0.

Postulate I. $\exists K$;

that is, there is an entity which belongs to the class.

Postulate II. $a \epsilon K . \supset . \exists K \frown b \ni [a \neq b]$;

that is, if a is an element of the class, there is an element b such that $a \neq b$.

Postulate $R1$. $a, b \epsilon K . a \neq b . \supset : a \circledcirc b . \smile . a \circledcirc b$;

that is, if a and b are elements of the class, and $a \neq b$, then either $a \circledcirc b$ or $a \circledcirc b$.

Postulate $R2$. $a, b \epsilon K . a \neq b . \supset : a \circledcirc b . a \circledcirc b . =. \Lambda$;

that is, if a and b are elements of the class, and $a \neq b$, then $a \circledcirc b$ and $a \circledcirc b$ cannot both be true.

Postulate $R3$. $a \epsilon K . \supset . a \circledcirc a . =. \Lambda$;

that is, if a is an element of the class, then $a \circledcirc a$ cannot be true.

Postulate $R4$. $a, b, c \epsilon K . a \neq c . a \circledcirc b . b \circledcirc c . \supset . a \circledcirc c$;

that is, if a, b, c are elements of the class, and $a \neq c$, then from $a \circledcirc b$ and $b \circledcirc c$ follows $a \circledcirc c$.

Postulate $R5$. $a, b \epsilon K : a \circledcirc b . \smile . a \circledcirc b : a \neq b : \supset :$

$$\exists K \frown x \ni [a \circledcirc x . x \circledcirc b] . \smile . \exists K \frown y \ni [a \circledcirc y . y \circledcirc b];$$

---

* See Burali-Forti. *Logica Matematica* (*Manuali Hoepli*, 1894), or the introductions to the several volumes of the *Formulaire de Mathématiques* (1895–1903). In reading statements written in these symbols, look first for the *dots*, which occur in groups of one, two, or more, and divide the sentence into its component parts; the larger the number of dots, the more important the point of division. Next find the symbol $\supset$, which is the sign of illation; thus, "$a . b . \supset . c$" means "*if* the propositions a and b are true, *then* the proposition c is true;" or, "the truth of propositions a and b *implies* the truth of propositions c." For the other symbols used in this paper, the following glossary will be sufficient:

"$a . \smile . b$" means "either a or b."

"$a \epsilon K$" means "a belongs to the class K;" "$a, b \epsilon K$" means "a and b both belong to the class K. (The "ϵ" is the initial letter of "$\grave{\epsilon}\sigma\tau\acute{\iota}$.")

"$\exists K$" means "there exists an element of the class K." "$\ni$" means "such that."

"$\exists K \frown a \ni$" means "there exists an element a, in the class K, such that."

"$\Gamma \epsilon$ Cls' K" means "Γ is a sub-class in the class K."

"$a . =. \Lambda$" means "the proposition a is false."

"Hp" means "hypothesis."

that is, if a and b are elements of the class such that $a \odot b$ or $a \otimes b$, then: if $a \neq b$, there is either an element x such that $a \odot x$ and $x \odot b$, or an element y such that $a \otimes y$ and $y \otimes b$.

POSTULATE *R*6. $\Gamma \epsilon \text{ Cls}' \; K . \; \exists \Gamma . \; \exists K \frown c \ni [\alpha \epsilon \Gamma . \supset . \alpha \odot c] . \supset .$

$$\exists K \frown X \ni [\alpha \epsilon \Gamma . \supset . \alpha \overline{\odot} X : x \epsilon K . \; x \odot X . \supset . \exists \Gamma \frown \xi \ni (\xi \otimes x)] :$$

that is, if Γ is a non-empty sub-class in K, and if there is an element c in K such that every element of Γ is $\odot c$, then there is an element X in K having the two following properties with regard to the sub-class Γ:

1°) if α is an element of Γ, then $\alpha \overline{\odot} X$; while

2°) if x is any element of K which is $\odot X$, there is an element in Γ which is $\otimes x$.

POSTULATE *A*1. $a, b \epsilon K . \supset . a \oplus b \epsilon K ;$

that is, if a and b are elements of the class, then $a \oplus b$ is an element of the class.

POSTULATE *A*2. $a, b, a \oplus b, b \oplus a \epsilon K . \supset . a \oplus b = b \oplus a ;$

that is, if a, b, $a \oplus b$, and $b \oplus a$ are elements of the class, then $a \oplus b = b \oplus a$.

POSTULATE *A*3. $a, b, c, a \oplus b, b \oplus c, (a \oplus b) \oplus c, a \oplus (b \oplus c) \epsilon K . \supset .$

$$(a \oplus b) \oplus c = a \oplus (b \oplus c) ;$$

that is, if a, b, c, $a \oplus b$, $b \oplus c$, $(a \oplus b) \oplus c$, and $a \oplus (b \oplus c)$ are elements of the class, then $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

POSTULATE *A*4. $a, x, y, a \oplus x, a \oplus y \epsilon K . \; a \oplus x = a \oplus y . \supset . x = y ;$

that is, if a, x, y, $a \oplus x$, and $a \oplus y$ are elements of the class, then from $a \oplus x = a \oplus y$ follows $x = y$.

POSTULATE *A*5. $\exists K . \supset . \exists K \frown z \ni (z \oplus z = z) ;$

that is, if there is any element in the class, then there is an element z such that $z \oplus z = z$.

POSTULATE *A*6. $\exists K \frown z \ni (z \oplus z = z) : z_1 \oplus z_1 = z_1 . z_2 \oplus z_2 = z_2 . \supset . z_1 = z_2 : a \epsilon K : \supset :$

$$\exists K \frown \bar{a} \ni (a \oplus \bar{a} = z) :$$

that is, if there is a uniquely determined element z such that $z \oplus z = z$, then for every element a there is an element $\bar{a}$ such that $a \oplus \bar{a} = z$.

POSTULATE *RA*1. Hp A6. $a, b, a \oplus b \epsilon K . \; a \otimes z . \; b \otimes z . \supset . a \oplus b \otimes a ;$

that is, if there is a uniquely determined element z such that $z \oplus z = z$; and if a, b, and $a \oplus b$ are elements of the class; and if $a \otimes z$ and $b \otimes z$; then $a \oplus b \otimes a$.

POSTULATE *RA*2. Hp A6. $a, b, a \oplus b \,\epsilon K.\ a \odot z.\ b \odot z.\ \supset.\ a \oplus b \odot a$:

that is, if there is a uniquely determined element z such that $z \oplus z = z$; and if a, b, and $a \oplus b$ are elements of the class; and if $a \odot z$ and $b \odot z$; then $a \oplus b \odot a$.

This completes the list of postulates in §3.

To show the mutual independence of these sixteen postulates—that is, to show that the list contains no redundancies—we exhibit, for each postulate, an interpretation of K, $\odot$, and $\oplus$ which satisfies all the other postulates, but not the one in question. Such postulate, then, cannot be a consequence of the other fifteen; for, if it were, every system $(K, \odot, \oplus)$ which had the other fifteen properties would have this property also, which is not the case.*

In constructing these systems, we assume the existence of the real numbers, as defined in the usual way by successive generalizations of the number-concept; and the symbols $<$, $+$, and 0 are used, in this section, only in their ordinary arithmetic meaning. The proof-systems are the following:

For I. $K =$ an "empty" class.

For II. $K =$ a class of a single element a. $a \odot a$ false. $a \oplus a = a$.

*For R*1. $K =$ all real numbers. $(a \odot b) = (a < b)$ when a and b are both positive or both negative; otherwise $a \odot b$ is false. $\oplus = +$.

*For R*2. $K =$ all real numbers. $(a \odot b) = (a \neq b)$. $\oplus = +$.

*For R*3. $K =$ all real numbers. $(a \odot b) = (a \leqq b)$. $\oplus = +$.

*For R*4. $K =$ a class of three elements, 0, 1, and 2. $0 \odot 1, 1 \odot 2, 2 \odot 0$. $a \oplus b = a + b$ when $a + b \leqq 2$, and $= a + b - 3$ when $a + b > 2$; in other words, $a \oplus b \equiv a + b \pmod 3$.

*For R*5. $K =$ all integral numbers. $\odot = <$. $\oplus = +$.

*For R*6. $K =$ all rational numbers. $\odot = <$. $\oplus = +$.

*For A*1. $K =$ all real numbers. $\odot = <$. $a \oplus b = a + b$ when $a + b = 0$, otherwise $a \oplus b =$ an entity not in the class.

*For A*2. $K =$ all real numbers. $\odot = <$. $a \oplus b = b$.

*For A*3. $K =$ all real numbers. $\odot = <$. $a \oplus b = 2(a + b)$ when a and b are both positive or both negative; otherwise $a \oplus b = a + b$.

*For A*4. $K =$ all real numbers. $\odot = <$. $a \oplus b = 0$ when $a \neq b$; and $a \oplus a = a$.

*For A*5. $K =$ all positive real numbers. $\odot = <$. $\oplus = +$.

*For A*6. $K =$ all positive real numbers, with 0. $\odot = <$. $\oplus = +$.

*For RA*1. $K =$ all real numbers. $(a \odot b) = (a > b)$ when a and b are both positive, otherwise $\odot = <$. $\oplus = +$.

*For RA*2. $K =$ all real numbers. $(a \odot b) = (a > b)$ when a and b are both negative, otherwise $\odot = <$. $\oplus = +$.

* This is the now familiar method of proving independence.

Thus the independence of the sixteen postulates of § 3 is established.

The independence of the ten postulates of § 1 is proved as follows:

For postulates I, II, $R1$–$R6$, use the systems just given, omitting the specifications in regard to $\oplus$.

For postulate $R7$, namely, $a, b \in K.\ a \neq b.\ \supset.\ \exists K \frown x \ni (x \odot a)$, use the system: $K =$ all real numbers between 0 and 1, with $0;\ \odot = <$.

For postulate $R8$, namely, $a, b \in K.\ a \neq b.\ \supset.\ \exists K \frown y \ni (y \odot a)$, use the system: $K =$ all real numbers between -1 and 0, with $0;\ \odot = <$.

To prove the independence of the eight postulates of § 2, use the systems above, omitting the specifications in regard to $\odot$.

§ 5. Further analysis of the postulates for group-theory.*

The set of eight postulates given in § 2 can be used only for *abelian* groups. In the present section I give a set of twelve postulates for groups in general, with a thirteenth postulate which makes the group abelian; and moreover (except in the case of postulate $G9$, which can probably be further sub-divided), each postulate has been made as nearly a *simple statement* as seems possible. †

Since the theory of groups has many applications not connected with real algebra, I represent the fundamental operation of the group, in the present set of postulates, by the symbol $\circ$, or by simple juxtaposition, instead of by the symbol $+$ or $\oplus$. Thus, $a \circ b$ (read: "a with b"), or ab, may be interpreted at pleasure as the "sum" of a and b, or the "product" of a and b, or the "resultant" of a and b, etc. I also represent the "zero-element," 0 or z, of § 2, by the symbol i ("identity"), which has a less special connotation. ‡

(The letter G is prefixed to the numbers of the postulates to suggest the word Group.)

Postulates I–II. The same as in § 2. Hence:

Theorem I. *There are at least two distinct elements in the class.*

Postulate $G1$. If a is an element of the class, then aa is an element of the class.

Postulate $G2$. If $a \neq b$, then ab is an element of the class. — Hence:

Theorem II. *If a and b are elements of the class, then ab is an element of the class.*

* Another set of postulates for groups will be presented in a subsequent paper.

† Most of the postulates embody, to be sure, a multitude of statements, corresponding to the multitude of elements in the group; but (except in case of $G9$) there seems to be no ground for distinguishing any of these statements from the rest; that is, there seems to be no ground for further subdivision of any of the postulates except $G9$. Cf. E. H. Moore, loc. cit.

‡ Compare footnote under postulate $A1$ in § 2.

POSTULATE $G3$. If there is any element in the class, there is an element i such that $ii = i$.

POSTULATE $G4$. If x and y are elements such that $xx = x$ and $yy = y$, then $x = y$. Hence:

Theorem III. *There is a uniquely determined element i such that $ii = i$.*

POSTULATE $G5$. If $ii = i$ and $aa \neq a$, then $ai = a$.

POSTULATE $G6$. If $ii = i$ and $aa \neq a$, then $ia = a$. Hence:

Theorem IV. *For every element a we have $ai = ia = a$.*

POSTULATE $G7$. If $ax = a$ and $aa \neq a$, then $xx = x$.

POSTULATE $G8$. If $xa = a$ and $aa \neq a$, then $xx = x$. Hence:

Theorem V. *If $ax = a$, or $xa = a$, then $x = i$.*

POSTULATE $G9$. If $aa \neq a$, $bb \neq b$, $cc \neq c$, and $ab \neq a$, $ab \neq b$, $bc \neq b$, $bc \neq c$; then

$$(ab)c = a(bc).$$

Hence:

Theorem VI. *For all elements $(ab)c = a(bc)$.* (Associative law.)

POSTULATE $G10$. If $ii = i$ and $aa \neq a$, then there is either an element a_r such that $aa_r = i$, or an element a_l such that $a_l a = i$.*

Now from $ax = i$ follows $xa = i$, and conversely. Thus, if $ax = i$, then $a(xa) = (ax)a = ia = a$, whence $xa = i$, by theorem V.

Further, if $ax = i$ and $ay = i$, then $x = y$. For, from $ax = i$ follows $yax = yi = y$, and from $ay = i$ follows $ya = i$ and $yax = ix = x$.

Hence, from postulate $G10$,

Theorem VII. *Every element a determines uniquely an element $\bar{a}$ such that $a\bar{a} = \bar{a}a = i$.*

Then if $ax = ay$, we have $\bar{a}ax = \bar{a}ay$, whence $x = y$; and similarly if $xa = ya$, we have $xa\bar{a} = ya\bar{a}$, whence $x = y$. Hence:

Theorem VIII. *A change in either a or b alone produces a change in ab.*

These twelve postulates, I–II, $G1$–$G10$, are thus sufficient to define a *group*. In order to make this group an *abelian* group, we must add another postulate, namely:

POSTULATE $G11$. If $aa \neq a, bb \neq b$, $ab \neq a, ab \neq b, ba \neq a$, and $ba \neq b$, then

$$ab = ba.$$

Hence:

Theorem IX. *For all elements, $ab = ba$.* (Commutative law.)

These thirteen postulates, I–II, $G1$–$G11$, are *independent* of each other, as is shown by the following systems, or interpretations of K and $\oplus$:

For I *and* II. The same systems as in § 4.

* This postulate was suggested by E. H. MOORE's six-postulate definition of a group; Transactions, vol. 3 (1902), p. 489; vol. 5 (1904), p. 549.

*For G*1. $K =$ all real numbers. $a \oplus b = a + b$ when $a \neq b$, or $a = 0$, or $b = 0$, or $a + b = 0$; otherwise $a \oplus b$ not in the class.

*For G*2. $K =$ all real numbers. $a \oplus b = a + b$ when $a = b$, or $a = 0$, or $b = 0$, or $a + b = 0$; otherwise $a \oplus b$ not in the class.

*For G*3. $K =$ all positive real numbers. $\oplus = +$.

*For G*4. $K =$ all positive real numbers. When $a \neq b$, $a \oplus b =$ the greater of the two numbers a and b; when $a = b$, $a \oplus a = a$.

*For G*5. $K =$ all positive real numbers with 0. $a \oplus b = a + b$, except that $a \oplus 0 = 0$.

*For G*6. $K =$ all positive real numbers with 0. $a \oplus b = a + b$, except that $0 \oplus a = 0$.

*For G*7. $K =$ all real numbers. $a \oplus a = 0$, $0 \oplus a = a \oplus 0 = a$; otherwise $a \oplus b = a$.

*For G*8. $K =$ all real numbers. $a \oplus b = 0$, $0 \oplus a = a \oplus 0 = a$; otherwise $a \oplus b = b$.

*For G*9. $K =$ all real numbers. $a \oplus b = 2(a + b)$, when a and b are both positive or both negative; otherwise $a \oplus b = a + b$.

*For G*10. $K =$ all positive real numbers with 0. $\oplus = +$.

*For G*11. Any non-abelian group with respect to $\oplus$. For example: $K =$ the class of all complex numbers (α, β) where α is positive and β real, with $\oplus$ defined so that $(\alpha_1, \beta_1) \oplus (\alpha_2, \beta_2) = (\alpha_1\alpha_2, \alpha_2\beta_1 + \beta_2)$. The complex numbers (α, β) may be represented by the points of the $\alpha\beta$-plane which lie to the right of the β-axis, the element i being the point $(1, 0)$.

§ 6. Another set of postulates for real algebra.

The set of postulates for groups given in § 5 suggests at once, (if we replace* ab by $a + b$ and i by 0), another set of postulates for real algebra, one which does not involve the commutative law,— namely the set consisting of the following twenty postulates:

Postulates I–II. (As in § 1 or § 2.)—These postulates give the class at least two distinct elements.

Postulates *R*1–*R*6. (As in § 1.)—These postulates, with I and II, make the class a *continuous scale*, or a *one-dimensional continuum*, with respect to the relation $<$.

Postulates *G*1–*G*10. (As in § 5.)—These postulates, with I and II, make the class a *group* (not necessarily an abelian group) with respect to the operation $+$.

Postulate *RG*1. If there is a uniquely determined element 0 such that $0 + 0 = 0$; and if a, b, $a + b$, and $b + a$ are elements of the class such that $a + b \neq a$, $a + b \neq b$, $b + a \neq a$, and $b + a \neq b$; then: if a and b are > 0, then $a + b$ is $> a$ and $> b$.

*Compare footnote under postulate *A*1 in § 2.

POSTULATE $RG2$. If the hypothesis of $RG1$ holds true, then: if a and b are $\prec 0$, then $a+b$ is $\prec a$ and $\prec b$.

These last two postulates serve to connect the symbols $\prec$ and $+$. In view of Postulates I, II, and $G1$–$G10$ [see especially theorem V in § 5] they give at once theorem 10 of § 3, namely: *If a and b are both above 0, then $a+b$ is above either of them; and if a and b are both below 0, then $a+b$ is below either of them.*

It remains only to prove the commutative law. From theorem 10 we have, as in § 3, theorems 13 and 15, and also:

Theorem 13a. *If $x>0$, then $x+a>a$; and if $x\prec 0$, then $x+a\prec a$;* and

Theorem 15a. *If $x\prec y$, then $x+a\prec y+a$, and conversely.*

From these theorems the principle of ARCHIMEDES can be deduced (as in theorem 23) without the aid of the commutative law, and hence that law itself can be proved by the method employed in my paper on the postulates of magnitude.*

Thus the equivalence of the sets of postulates in § 3 and § 6 is established.

The *independence* of the twenty postulates of this set (§ 6) is shown by the following systems:

For I–II, *and* $R1$–$R6$. The same systems as in § 4.

For $G1$–$G10$. The systems used in § 5, with $\odot$ defined as $\prec$.

For $RG1$ *and* $RG2$. The systems used for $RA1$ and $RA2$ in § 4.

An unsolved problem.†

I conclude this section with the statement of the following problem: Suppose that the postulates $RG1$ and $RG2$ in § 6 are "weakened" so as to read "$\cdots > a$ OR $> b$" and "$\cdots \prec a$ OR $\prec b$," instead of "$\cdots \prec a$ AND $\prec b$" and "$\cdots \prec a$ AND $\prec b$"; is the commutative law then still deducible, or is postulate $G11$ an independent postulate?

In attempting to prove the latter alternative, two "proof-systems" suggest

* Transactions, vol. 3 (1902), pp. 270–271. The method is due to O. HÖLDER.—The same method is used by BURALI-FORTI (*Teoria generale* ···, loc. cit.) in deducing the commutative law from a set of eight postulates for the class of positive real numbers with 0. In order, however, to make his proof of the principle of ARCHIMEDES convincing, certain modifications are necessary. In a letter of November 11, 1904, he proposes, therefore, the following corrected form of his definition 1·3, page 6, and his postulate VI, page 7:

$\cdot 3.\ a\varepsilon u.\ \supset.\ \theta(u,f)a = u\frown x_3\{a\varepsilon\{xf(u\text{-Nul}(u,f))\smile(u\text{-Nul}(u,f))fx\}\}$ Df

$[\text{VI}]\,x,\ y\varepsilon u.\ \supset_{x,y}: x=y.\smile.\ x\varepsilon\theta(u,f)y.\smile.\ y\varepsilon\theta(u,f)x.\cdot$

With these changes, his proofs of the principle of ARCHIMEDES and the commutative law present no further difficulty.

† This problem is closely connected with the unsolved problem No. 1 in my paper on magnitudes, Transactions, vol. 3 (1902), p. 279.

themselves. First, we might try the system used for $G11$ in § 5, with $\circledcirc$ defined as follows: $(\alpha_1, \beta_1) \circledcirc (\alpha_2, \beta_2)$ when $\alpha_1 < \alpha_2$, or when $\alpha_1 = \alpha_2$ and $\beta_1 < \beta_2$. This system satisfies $RG1$ and $RG2$, but fails for $R6$ (on continuity). Again, we might try the same system as to K and $\oplus$, with $\circledcirc$ defined as follows: bring the points (α, β) of the half-plane into one-to-one correspondence with the points of a straight line as G. CANTOR has shown how to do;* and then interpret $\circledcirc$ as "below" (or "on the left of"). This system satisfies all the postulates $R1$–$R6$, but it is not easy to see how to make it satisfy *both* of the postulates $RG1$ and $RG2$.—The independence of postulate $G11$, in the revised set of postulates proposed in the problem, is therefore an open question.

§ 7. A CONDENSED LIST OF POSTULATES.

In the previous sections I have attempted to analyze the fundamental propositions of real algebra into their simplest (independent) component statements, and the number of postulates in each list is therefore large. In the present section, on the other hand, I give a condensed list of postulates, in which the number is much smaller. The list comprises the following ten postulates:

1. There are at least two distinct elements in the class.
2. If $a < b$ and $b < c$, then $a < c$.
3. $a < a$ is false.
4. If $a \neq b$, then there is either an element x such that $a < x$ and $x < b$, or an element y such that $a > y$ and $y > b$.
5. If Γ and Γ' are two non-empty sub-classes in K, such that every element of Γ is $<$ every element of Γ', then there is at least one element, M, which is $\geqq$ every element of Γ and $\leqq$ every element of Γ'.
6. If a and b are elements of the class, then $a + b$ is an element of the class.
7. $a + b = b + a$, whenever the sums involved are elements of the class.
8. $(a + b) + c = a + (b + c)$, whenever the sums involved are elements of the class.
9. If a, b, and $a + b$ are elements of the class, there is an element x such that $a = b + x$.
10. If $x < y$ then $a + x < a + y$, whenever the sums involved are elements of the class.

The sufficiency of these ten postulates is shown as follows:

From postulates 2 and 3 we have: $a < b$ and $a > b$ cannot both be true. From postulates 2 and 4 we have: if $a \neq b$, then either $a < b$ or $a > b$. Postulates 4 and 5 give density and continuity. Hence by § 1, postulates 1–5

* G. CANTOR, *Ein Beitrag zur Mannigfaltigkeitslehre*, CRELLE'S Journal für die reine und angewandte Mathematik, vol. 84 (1877), pp. 242–258; translated under the title *Une contribution à la théorie des ensembles*, Acta Mathematica, vol. 2 (1883), pp. 311–328.

make the class a *continuous scale*, or a *one-dimensional continuum*, with respect to $<$. Further, postulates 6–9 make the class an *abelian group* * with respect to $+$; and postulate 10 gives theorem 10 of § 3.

Hence the set of ten postulates in § 7 defines the same algebra as the set of sixteen postulates in § 3.

The *independence* of postulates 1–10 is shown as follows: For 1–5, and 7–10, use the systems given in § 4 for postulates II, $R4$, $R3$, $R5$, $R6$, and $A2$, $A3$, $A5$, $RA1$, respectively. For 6, use the system: $K =$ all real numbers; $\circ = <$; $a \oplus b = a + b$ when a and b are integers; otherwise $a \oplus b$ not in the class.

HARVARD UNIVERSITY, CAMBRIDGE, MASS.,
September, 1904.

APPENDIX. A SET OF POSTULATES FOR REAL ALGEBRA, IN WHICH MULTIPLICATION IS INCLUDED AS A FUNDAMENTAL CONCEPT.

In the preceding sections of this paper, multiplication has been thought of as a derived concept, the product of two elements with respect to an arbitrarily chosen (positive) unit-element being definable in terms of the fundamental concepts $<$ and $+$. In this appendix, on the other hand, multiplication is regarded as itself a fundamental concept, whose properties are determined by postulates.

We consider, namely, a class, K, a relation, $<$ (read: "below" or "before") and *two* operations, $+$ and $\times$ (read: "plus" and "times"), and inquire what conditions must be imposed upon the system $(K, <, +, \times)$ to make it equivalent to the algebra of a real variable with respect to $<$, $+$, and $\times$. These conditions are expressed in the following twenty postulates (the letters R, A, and M indicating the postulates which concern the Relation $<$, the operation of Addition, and the operation of Multiplication, respectively):

POSTULATES I, II, $R1$–$R6$, $A1$–$A6$, $RA1$–$RA2$. The same as in § 3.

POSTULATE $M1$. If a and b are elements of the class, then $a \times b$ (or ab) is an element of the class.

POSTULATE $M2$. If a, b, ab, and ba are elements of the class, then $ab = ba$. (Commutative law for multiplication.)

POSTULATE $AM1$. If $a, b, c, b + c, ab, ac, a(b + c)$, and $(ab) + (ac)$ are elements of the class, then $a(b + c) = (ab) + (ac)$. (Distributive law for multiplication with respect to addition.)

POSTULATE $RAM1$. If 0 is a uniquely determined element such that

* E. V. HUNTINGTON, Transactions, vol. 4 (1903), p. 27. But note that E. H. MOORE's query as to "definition W_1'," in Transactions, vol. 3 (1902), p. 489, is not yet completely answered.

$0 + 0 = 0$, and if a, b, and ab are elements of the class, and $a > 0$ and $b > 0$, then $ab > 0$.

From these postulates we have:

Theorem 31. $c \times 0 = 0 \times c = 0$ *for every element* c.

Theorem 32. $a \times (-b) = (-a) \times b = -(a \times b)$.

Theorem 33. *If* a *and* b *are both positive or both negative,* ab *is positive; if either is positive and the other negative,* ab *is negative.* (See definitions under theorem 12.) Hence:

Theorem 34. *If* $a \neq 0$ *and* $b \neq 0$, *then* $ab \neq 0$.

If now we select at pleasure a positive element E, and notice that every positive element a is the upper limit of the class of all the rational fractions of E which are $< a$ (see definitions under postulate $R6$ and theorem 27), we can prove the associative law for multiplication (first for positive elements, and then, by the aid of theorem 32, for all elements), and also the possibility of "division" when the divisor is different from zero; that is:

Theorem 35. $(ab)c = a(bc)$; and

Theorem 36. *For every two elements* a *and* b, *provided* a *is not zero, there is an element* x *such that* $ax = b$.

Thus we see that the elements of K *excluding zero* from an *abelian group* with respect to $\times$. [Hence:* 1°) there is a uniquely determined "unit-element," 1, not zero, such that $1 \times 1 = 1$; 2°) for every element a, $1 \times a = a \times 1 = a$; and 3°) if $a \neq 0$, then from $ax = ay$ follows $x = y$.] Therefore the whole system is a *field*† with respect to $+$ and $\times$.

Making use again of classes of rational fractions, we can now prove:

Theorem 37. *Any two systems,* $(K, <, +, \times)$ *and* $(K', <, +, \times)$, *which satisfy the twenty postulates of this appendix are* EQUIVALENT *with respect to* $<$, $+$ *and* $\times$; *that is, they can be brought into one-to-one correspondence in such a way that*

1°) *from* $a < b$ *follows* $a' < b'$, *and conversely;*

2°) *from* $a + b = c$ *follows* $a' + b' = c'$, *and conversely; and*

3°) *from* $ab = c$ *follows* $a'b' = c'$, *and conversely;—*

where a', b', c' *are the elements in* K' *which correspond to the elements* a, b, c *in* K. *Further, this correspondence can be established in only one way, since the "unit-element" is fixed in each system.*

The last clause of the theorem, namely that the correspondence can be established in only one way, marks the essential distinction between the postulates of the appendix (expressed in terms of $<$, $+$, and $\times$) and the postulates of

*Cf. Transactions, vol. 4 (1903), pp. 27–28.

†Cf. L. E. Dickson and E. V. Huntington, Transactions, vol. 4 (1903), pp. 13 and 31. Notice that postulates I, II, $A1$–$A6$, $M1$–$M2$, $AM1$ are not sufficient to define a field, without the aid of the postulates concerning $<$ (as witness the system of all integers with respect to $+$ and $\times$). A further discussion of the postulates for a field will be presented in a later paper.

§ 3 (expressed in terms of $\prec$ and $+$). For in § 3 the correspondence could be established in an infinite number of ways, according to the infinite number of ways in which the "unit-elements" might be selected. The postulates of the appendix, therefore, determine the algebra *uniquely* in a stronger sense than do the postulates of the preceding sections.

As examples of systems $(K, \circledcirc, \oplus, \odot)$ which satisfy all the postulates, and to illustrate theorem 37, I mention the following "equivalent" systems (the symbols $\prec$, $+$, and $\times$, being now used in their ordinary arithmetical meanings):*

1) K = all real numbers; $\circledcirc = \prec$; $\oplus = +$; $\odot = \times$. (Here $z = 0$, $u = 1$.)

2) K = all real numbers > 0; $\circledcirc = \prec$; $a \oplus b = ab$; $a \odot b = \exp(\log a \cdot \log b)$. (Here $z = 1$, $u = e$ = base of the system of logarithms.)

3) K = all real numbers > 1; $\circledcirc = \prec$; $a \oplus b = \exp(\log a \cdot \log b)$; $a \odot b = \exp\{\exp[\log(\log a) \cdot \log(\log b)]\}$. (Here $z = e$, $u = e^e$.)

4) K = all real numbers; $\circledcirc = \prec$; $a \oplus b = (a^{\frac{1}{3}} + b^{\frac{1}{3}})^3$; $a \odot b = ab$. (This example was suggested to me by Professor BOUTON.)

The existence of any such system proves the *consistency* of the postulates.

It remains to show that the twenty postulates of the appendix are *independent*; that is, to exhibit twenty interpretations of K, $\circledcirc$, $\oplus$, and $\odot$, in which all the other postulates are satisfied, but not the one in question. These proof-systems are the following:

For I. K = an "empty" class.

For II. K = a class of a single element a. $a \circledcirc a$ false. $a \oplus a = a$. $a \odot a = a$.

For $R1$–$R6$, $A1$–$A6$, $RA1$–$RA2$. The systems used in § 4, with $\odot$ defined as ordinary multiplication, except that in the system for $R4$ the product is taken modulo 3.

For the remaining postulates, use the system of all real numbers, with $\circledcirc$ and $\oplus$ defined as the ordinary $\prec$ and $+$, and $\odot$ defined as follows:

For $M1$. $a \odot b = ab$ when a and b are both rational, otherwise $a \odot b$ not in the class.

For $M2$. $a \odot b = b$.

For $AM1$. $a \odot b = a + b$.

For $RAM1$. $a \odot b = -ab$.

Thus the independence of the twenty postulates is established.

We notice in conclusion that we may replace the first sixteen postulates of this list by the twenty postulates of § 6, or by the ten postulates of § 7, thus forming two new sets of twenty-four and fourteen postulates, respectively. The independence of the postulates of each of these sets is readily verified, by the aid of the proof-systems already employed.

* See the opening paragraph in § 1 and § 2. For convenience in printing, $\exp x$ is written for e^x.

ON THE PRIMITIVE GROUPS OF CLASS $3p$*

BY

W. A. MANNING

In this paper are considered only those groups which contain a substitution of order p and degree $3p$, p an odd prime. Two general theorems are first established and then class 9 is disposed of before the general problem is considered.

THEOREM I. *Let A be a substitution of degree pq and order p in a group of class pq, $q \leqq p$. No substitution similar to and non-commutative with A can be free from all the letters of any one cycle of A. An exception may occur when $q = p$ and the group contains a transitive subgroup of order p^2.*

Let B be a substitution similar to A, non-commutative with A, and free from all the letters of r cycles of A. If $q < p$, no two substitutions similar to A can displace exactly the same letters unless one is a power of the other,† and we may assume this to be true in the groups of class p^2 here considered, since the knowledge that G contains a transitive subgroup of degree p^2 makes its consideration and determination relatively simple.

If B does not connect old and new letters transitively in its cycles, $A^{-1}B^{-1}AB$ is of degree not greater than $(q-r)p$, and is not the identity. We can now assume that B and all its powers connect old and new letters transitively.

It will be shown that a substitution F can always be found among the substitutions similar to A, which transforms into themselves the r cycles of A left fixed by B and which displaces not more than $q-r$ letters new to A. The existence of F depends only upon the existence of B and leads to a substitution, not the identity, which displaces at most $(q-r)p+q-r$ letters. If B displaces not more than q new letters and $q \neq p$, we have at once a substitution $A^{-1}B^{-1}AB$ of degree less than pq. If $q = p$, an apparent exception arises when $r = 1$, and B displaces just p new letters. But here $A^{-1}BA$ is not a power of B and displaces the same p^2 letters as B.

It is now assumed that B displaces more than q new letters, so that some cycle contains at least two new letters. In $B^{-\rho}AB^{\rho} = C$, suppose ρ so chosen that two new letters which occur in the same cycle of B are adjacent in B^{ρ}.

* Presented to the Society (San Francisco) April 25, 1903. Received for publication June 2, 1904.

† Transactions of the American Mathematical Society, vol. 4 (1903), p. 351.

The substitution C does not displace as many new letters as B and in it r cycles of A occur unchanged. C certainly contains one or more new letters. We now wish to show that the new letters which are in C cannot merely fill up isolated cycles of C, but that C also must connect old and new letters in its cycles. Let $C = C_1 SR$, where C_1 contains only old letters, S only new ones, and R is made up of the r unchanged cycles of A. Let S have s cycles. Break A up into two parts, $A = A_1 R$, where $A_1 = c_1 c_2 \cdots c_{q-r}$. The substitution $A^{-1}C = (A_1^{-1}C_1)S$ contains not more than $(q-r+s)p$ letters. Unless $s \geqq r$, G is of class less than pq. Again $A^{-1}C^{-1}AC = A_1^{-1}C_1^{-1}A_1C_1$ lowers the class of G to $(q-r)p$ or less unless we have $A_1^{-1}C_1A_1 = C_1$. This condition can be satisfied only if $C_1 = c_1^{r_1}c_2^{r_2}\cdots c_{q-r-s}^{r_{q-r-s}}$, since C_1 has at most $p-2$ cycles. From this form of C it follows that if a letter of any cycle of A is left fixed by B^ρ, no letter of that cycle occurs in B. But by hypothesis B is free from just r complete cycles of A. Then B^ρ contains just $(q-r)p$ old letters. The number of new letters in B^ρ is $sp = rp$, and since these rp new letters are all found in C, each one of them is in B^ρ preceded by an old letter. But ρ was chosen so that two new letters would be adjacent in B^ρ. We conclude that C connects old and new letters transitively.

Suppose that in some cycle of C two or more new letters are found. Again we choose ρ so that two new letters are adjacent in C^ρ. Then $D = C^{-\rho}AC^\rho$ displaces fewer new letters than does C, retains unchanged the r cycles of A left fixed by B, and furthermore connects old and new letters. The last statement requires proof.

In case D does not connect old and new letters, $D = D_1 SR$, where D_1 contains old letters only; S, sp new letters only; and R repeats r cycles of A without change. The degree of $A^{-1}D = (A_1^{-1}D_1)S$ is not greater than $(q-r+s)p$; hence $s \geqq r$. Again $A^{-1}D^{-1}AD = A_1^{-1}D_1^{-1}A_1D_1 = 1$, since this substitution cannot displace more than $(q-r)p$ letters. Hence $D_1 = c_1^{r_1}\cdots c_{q-r-s}^{r_{q-r-s}}$. Now $C^{-\rho}AC^\rho = D = c_1^{r_1}\cdots c_{q-r-s}^{r_{q-r-s}}SR$. It follows that if a letter of any cycle of A is missing from C^ρ, no letter of that cycle occurs in C. Therefore C leaves fixed all the letters of at least s cycles of A. But we have seen that $s \geqq r$. The same reasoning can now be applied to C as was applied to B. Then D has the properties stated. Applying the same method to D we obtain another substitution E similar to A, connecting old and new letters transitively, containing unchanged at least r cycles of A, and displacing fewer new letters than D. This process can be continued until a substitution F is reached which has at least r cycles of A unchanged, is similar to A, and introduces k $(q-r \geqq k \geqq 1)$ new letters with no two new letters in the same cycle. The substitution $A^{-1}F$ displaces not more than $(q-r)p + q - r$ letters, which is contrary to the hypothesis that $r \geqq 1$.

THEOREM II. *Among the substitutions similar to A in a primitive group of class pq $(1 < q \leqq p)$, p odd, a substitution B can be found connecting transitively two cycles of A and having not more than one new letter in any cycle.*

Since G is primitive the similar substitutions $A, \cdots$ generate a transitive group. If no one of the set replaces all the letters $a_1, a_2, \cdots, a_p$ by other letters, one of them connects two cycles of A and has not more than one new letter α in any cycle.* But if A_1 replaces all the letters $a_1, \cdots$ by other letters, these p letters a are found in at least three of the q cycles of A_1, so that by the theorem just proved some cycle of A_1 contains letters from different cycles of A. Therefore there always is in the set $A, \cdots$ a substitution $B = (a_1 b_1 \cdots) \cdots$.

Among all the substitutions $A, \cdots$ which connect cycles of A, there is one which displaces a minimum number λ of the new letters α. It is immaterial which two cycles of A are connected. Let B be a substitution of the form $(ab \cdots) \cdots$ displacing λ new letters. Also let B leave fixed one of the letters a. It cannot have two new letters α consecutive, for then $B^{-1}AB$ would connect letters a and b in one of its cycles and would displace fewer than λ new letters. Suppose that B has two or more new letters in its first cycle. A convenient power B^ρ makes these two new letters consecutive. In B^ρ letters a can only be followed (or preceded) by other letters a and new letters α. Hence in the first cycle of B^ρ there are the sequences $a'\alpha'$ and $b'\alpha''$, where a' is one of the letters $a_1, \cdots, a_p$, and b' is one of the remaining $(q-1)p$ letters of A. Now choose σ so that $B^{\rho\sigma} = (a'b' \cdots \alpha'\alpha'' \cdots) \cdots$. Since by hypothesis B leaves an a fixed, $B^{-\rho\sigma} A B^{\rho\sigma}$ connects cycles of A and has fewer than λ letters α. Then B has just one α in its first cycle. It is clear that any power of B has a letter a followed (or preceded) in its first cycle by a letter from another cycle of A. Hence B cannot have two new letters in any cycle.

We shall now show that it may always be assumed that B leaves a letter a fixed. Suppose that B displaces all the $a_1, \cdots, a_p$. Evidently the same is true of $b_1, b_2, \cdots, b_p$. If the $2p$ letters $a_1, \cdots, b_i, \cdots$ occupy just two cycles of B, any power of B replaces some a by an a and some other a by a b, and, as before, B has not more than one new letter α to a cycle. If the $2p$ letters $a_1, \cdots, b_1, \cdots$ are found in more than two cycles of B, two cases arise. First, let no letter $c, d, \cdots$ be in the same cycle with an a or b. Some power B^κ of B now connects c and d, say, because of Theorem I. Then B must displace the $2p$ letters $c_1, \cdots, d_1, \cdots$, and these letters again are found in at least two cycles of B. Now if no e is in a cycle of B with c or d, we have a B^η connecting e and f, with the same conditions. Proceeding thus we finally find that either B connects two cycles k and l of A, leaving fixed some of the letters $k_1, \cdots, k_p$, or else B connects three or more cycles of A. So we have the second case,

*JORDAN, Journal für Mathematik, vol. 79 (1874), pp. 249-253.

a letter c is in a cycle with a and b. Here B displaces the $3p$ letters $a_1, \cdots, b_1, \cdots, c_1, \cdots$. These $3p$ letters cannot occupy just 3 cycles of B, for then any power of B would transform A into a new substitution connecting cycles of A. In fact B cannot have kp letters of k cycles of A in k cycles by themselves for the same reason. Hence $a_1, \cdots, b_1, \cdots, c_1, \cdots$ are to be found in at least 4 cycles of B. Continuing thus it is evident that B either displaces all the qp letters of A or connects two cycles of A without displacing all the letters of one of the two cycles.

Class 9.

Let there be a transitive subgroup (F) of degree 9 in G. This subgroup cannot be cyclic for it would then be contained in a doubly transitive G^{10},* which does not exist. If F is non-cyclic it leads to a doubly transitive $G^{13}_{13.12.9}$, also impossible.

We can now say that there is a substitution B similar to A which connects transitively two cycles of A and displaces one, two, or three new letters.

Suppose that $I_1 = \{A, B\}$ is intransitive. It is a simple isomorphism between two transitive constituents, one of which is of degree 4 and order 12. Now the other constituent can only be of degree 6, and class 4, lowering the class of G to 8.

Then I_1 is transitive. It is of degree 12 and order 36. The 4 systems of imprimitivity of three letters each can be chosen in only one way. Hence I_1 must be maximal in a doubly transitive $G^{13}_{13.12.3}$, an absurdity. No primitive group of class 9 exists.

Class $3p$, $p > 3$.

If a primitive group contains a cyclic subgroup F on $3p$ letters, it also contains a doubly transitive $G^{3p+1}_{(3p+1)3p}$. Then $3p = 2^{2m} - 1$, and $p = 5$. We have here a $G^{16}_{16.15}$† which is maximal in turn in a G^{17}, but is not contained in a 4-ply transitive group of degree 18.‡

In case F is non-Abelian only the doubly transitive G^{3p+1} need be examined. Here the subgroup transforming F into itself has a tetrahedral subgroup in its quotient group. But such a subgroup is not to be found in the group of isomorphisms of F.

Let $I_1 = \{A, B\}$, of degree greater than $3p$, be intransitive, and let I_1' and I_1'' be the two simply isomorphic transitive constituents of degrees $2p + k'$,

* JORDAN, Journal de Mathématiques, ser. 2, vol. 16 (1871), p. 383; MARGGRAFF, *Ueber primitive Gruppen mit transitiven Untergruppen geringeren Grades*, Dissertation, Giessen, 1889.

† MILLER, *The primitive groups of degree* 16, American Journal of Mathematics, vol. 20 (1898), p. 229; *The transitive groups of degree* 17, Quarterly Journal of Mathematics, vol. 31 (1899), p. 49.

‡ JORDAN, Journal de Mathématiques, ser. 2, vol. 17 (1872), p. 351.

$p+k''$, respectively; where $k', k''=0, 1$; $k'=k''\neq 0$. Suppose I_1'' of degree p. It is then of class $p-2$, and hence* is the simple triply transitive $G_{p,p-1,p-2}$. To all the substitutions not of order p in I_1'' must correspond substitutions of degree $2p+2$ in I_1. Hence $(p-1)(p-2)=2p+2$, from which $p=5$. The group I_1 is icosaedral of degree 17. Next suppose that I_1'' is of degree $p+1$. It can only be of class $p-1$ and hence is of order $(p+1)p\cdot 2$. Now I_1'' has $(p+1)p/2$ subgroups of order 2 on $p-1$ letters, and each is invariant in a subgroup of order 4. But the substitutions of order 2 involve all possible transpositions of $p+1$ letters, so that a given transposition is found in $(p-1)/2$ distinct substitutions. These $(p-1)/2$ substitutions generate an Abelian group since the product of any two of them is of order 2. Hence $(p-1)/2=2$, $p=5$.†

Since the degree of I_1' exceeds $(3p-1)/2$ a substitution C similar to A can be found in G which connects I_1' and I_1'', and introduces at most three letters new to I_1.

We take up I_{60}^{17} first. A transitive group of degree 17 and class 15 is triply transitive and has already been considered. It may be remarked that I_{60}^{17} cannot be included in a larger intransitive group of the same degree. Then $I_2=\{A, B, C\}$, if of degree 18, is of order $18\cdot 60$. This group cannot be primitive, as may be shown as follows. There are in I_2 36 conjugate subgroups of order 5, each of which is invariant in a subgroup of order 30. By considering the transitive representation of I_2 on 36 letters it is seen that I_2 has one conjugate set of 6 subgroups of order 3, and since no operator of order 5 can be permutable with each of the 6 subgroups of order 3, I_2 is isomorphic to a multiply transitive group on 6 letters. Then I_2 has either an invariant intransitive subgroup or a regular invariant subgroup of order 18 containing negative substitutions. But I_2 is a positive primitive group by hypothesis. Since I_2 is generated by I_1^{17} and C, it cannot be imprimitive. Continuing in much the same way the examination of the limited number of cases to which I_{60}^{17} and I_{60}^{18} lead, we reach the conclusion that the subgroup I_1 of G is never intransitive.

If the transitive group I_1 is of degree $3p+1$ it is primitive of order $(3p+1)p$. Here again $p=5$, because of the condition $3p+1=2^\alpha$. This well-known G_{80}^{16} is not maximal in a group of degree 17. If I_1 is of degree $3p+2$, the number of subgroups of order p in it is $(3p+2)/2$, an absurdity. Let $I_1=\{A, B\}$ be of degree $3p+3$. Since any substitution of I_1 which replaces one new letter by another must merely permute the new letters among themselves, I_1 is imprimitive. There are $p+1$ systems of 3 letters each. Since a system of three letters can be chosen in only one way, I_1 leads to a

*Cf. MAILLET, *Recherches sur les Substitutions*, etc., Dissertation, Paris, 1892, p. 78.

†Cf. DE SÉGUIER, Comptes Rendus de l'Académie des Sciences de Paris, vol. 137 (1903), p. 37.

doubly transitive G^{3p+4} of order $(3p+4)(3p+3)p$ or $(3p+4)(3p+3)2p$. In G the Sylow subgroup of order p is invariant in a group in which the quotient-group is tetrahedral or octahedral. This is impossible.

There exist then only three primitive groups of class $3p$, p odd, containing a substitution of order p and class $3p$. These groups are of class 15 and order 80, 240 and 4080.

THE MINIMUM DEGREE τ OF RESOLVENTS FOR THE p-SECTION OF THE PERIODS OF HYPERELLIPTIC FUNCTIONS OF FOUR PERIODS*

BY

LEONARD EUGENE DICKSON†

Introduction.

The chief object of the investigation‡ is to prove that, if $p > 3$,

$$\tau = (p^4 - 1)/(p - 1).$$

The case $p = 3$ alone is exceptional, the problem then being equivalent to that of the 27 lines on a general cubic surface. On the final page of his *Traité*,§ JORDAN states that he had established the theorem for $p = 5$, by methods analogous to those used in his complicated discussion for $p = 3$, and says "mais ici la complication est beaucoup plus grande."

It is rather remarkable that the minimum τ should be so large as $p^3 + p^2 + p + 1$, since the fractional form of the general quaternary linear group modulo p can be represented as a substitution group of this degree (and of no lower in view of the present theorem).

The paper makes considerable headway in the problem of all the subgroups of the quaternary abelian group modulo p, which plays the same rôle in the hyperelliptic modular theory (as yet but little developed) as the binary congruence group plays in the classic elliptic modular theory.

Properties of three maximal subgroups of $SA(4, p^n)$.

1. We consider special abelian‖ transformations of the three types

* Presented to the Society (Chicago), December 30, 1904. Received for publication November 17, 1904.

† Of the Carnegie Institution of Washington.

‡ A sequel to my series of articles in these Transactions. Occasional reference to them is made by Roman numerals as in the list in the paper, *Determination of all the subgroups of the known simple group of order* 25920, in vol. 5 (1904), p. 127.

§ Note *E*, p. 667. Also in Comptes Rendus (1870), p. 1028.

‖ The abelian conditions on $(1)_1$ and $(1)_2$ are given by (7) of II_{374} and (19) of II_{280}, respectively. The sign $\pm$ preceding the matrices in II is now to be omitted.

$$(1)\qquad \begin{pmatrix} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ 0 & \alpha_{11}^{-1} & 0 & 0 \\ 0 & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ 0 & \delta_{21} & \beta_{22} & \delta_{22} \end{pmatrix}, \quad \begin{pmatrix} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ 0 & \delta_{11} & 0 & \delta_{12} \\ \alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ 0 & \delta_{21} & 0 & \delta_{22} \end{pmatrix}, \quad \begin{pmatrix} \alpha_{11} & \gamma_{11} & 0 & 0 \\ \beta_{11} & \delta_{11} & 0 & 0 \\ 0 & 0 & \alpha_{22} & \gamma_{22} \\ 0 & 0 & \beta_{22} & \delta_{22} \end{pmatrix}.$$

Those of type $(1)_1$ form a group G_ω of order $\omega = (p^{2n}-1)(p^n-1)p^{4n}$. The operators with $\alpha_{11}=1$ form a subgroup $G_{\omega'}$ of order $\omega' = (p^{2n}-1)p^{4n}$. Next, the operators of type $(1)_2$ form a group H_ω; those with $\alpha_{11}\alpha_{22}-\alpha_{12}\alpha_{21}=1$ form a subgroup $H_{\omega'}$. Finally, there are $\{(p^{2n}-1)p^n\}^2$ operators $(1)_3$ with

$$(2)\qquad \alpha_{11}\delta_{11}-\beta_{11}\gamma_{11}=1, \qquad \alpha_{22}\delta_{22}-\beta_{22}\gamma_{22}=1.$$

These and their products by $P_{12}=(\xi_1\xi_2)(\eta_1\eta_2)$ form a group K_π, $\pi = 2(p^{2n}-1)^2p^{2n}$. A subgroup $K_{\pi'}$, $\pi' = (p^{2n}-1)p^{2n}$ is formed of the operators

$$(3)\quad \xi_1' = \xi_1 + \gamma_{11}\eta_1, \qquad \eta_1' = \eta_1, \qquad \xi_2' = \alpha_{22}\xi_2 + \gamma_{22}\eta_2, \qquad \eta_2' = \beta_{22}\xi_2 + \delta_{22}\eta_2.$$

2. THEOREM. *If a subgroup of $SA(4, p^n)$ contains $G_{\omega'}$, it lies in G_ω. In particular, G_ω is a maximal subgroup.*

We extend $G_{\omega'}$ by a transformation S of $SA(4, p^n)$, not in G_ω, and prove that the group obtained is $SA(4, p^n)$. Give to S the notation (1) of II_{372}. By hypothesis, $\beta_{11}, \beta_{12}, \delta_{12}$ are not all zero. We may assume that β_{11} and β_{12} are not both zero, otherwise $M_2 S$ has $\beta_{12}' = -\delta_{12} \neq 0$, while M_2 lies in G_ω.

Let first $\beta_{11}=0$, $\beta_{12}\neq 0$. Employing S^{-1} if necessary, we may take $\beta_{11}=0$, $\beta_{21}\neq 0$. Then $S' \equiv SN_{1,2,\rho}$, where $\alpha_{11}+\rho\beta_{21}=1$, is of the form S with $\alpha_{11}=1$, $\beta_{11}=0$, $\beta_{21}\neq 0$. Now $G_{\omega'}$ contains a transformation T which leaves η_1 fixed and replaces ξ_1 by the same function $\xi_1 + \cdots$ that S' does. Then $S_1 \equiv T^{-1}S'$ leaves ξ_1 fixed and has $\beta_{11}=0$. The abelian conditions give

$$\delta_{11}=1, \qquad \gamma_{21}=\delta_{21}=0, \qquad \alpha_{22}\delta_{22}-\beta_{22}\gamma_{22}=1.$$

The product $S_2 \equiv S_1U^{-1}$, where $U=\left(\begin{smallmatrix}\alpha_{22} & \gamma_{22}\\ \beta_{22} & \delta_{22}\end{smallmatrix}\right)$ on ξ_2 and η_2, is

$$\xi_1'=\xi_1, \qquad \eta_1'=\eta_1+\beta_{12}\xi_2+\delta_{12}\eta_2, \qquad \xi_2'=\xi_2+\alpha_{21}\xi_1, \qquad \eta_2'=\eta_2+\beta_{21}\xi_1.$$

By the hypothesis on S, S_2 is not in G_ω, so that β_{12} and δ_{12} are not both zero. Now $G_{\omega'}$ contains an operator V which leaves ξ_1 and η_1 unaltered and replaces ξ_2 by $-\kappa^{-1}(\beta_{12}\xi_2+\delta_{12}\eta_2)$, where κ is any mark $\neq 0$. Then $V^{-1}S_2V = R_{1,2,\kappa}$. Now M_1^{-1} transforms the latter into $Q_{2,1,\kappa}$. But $G_{\omega'}$ contains $Q_{1,2,\kappa}$. Hence we reach

$$(4)\qquad P_{12} = Q_{2,1,1}^{-1}Q_{1,2,1}Q_{2,1,1}^{-1}T_{2,-1}, \qquad M_1 = P_{12}M_2P_{12},$$

and hence (*Linear Groups*, p. 92) all the generators of $SA(4, p^n)$.

Let next $\beta_{11} \neq 0$. Then $S' \equiv N_{1,2,-\delta_{12}\beta_{11}^{-1}} Q_{1,2,-\beta_{12}\beta_{11}^{-1}} S$ replaces η_1 by $\beta_{-1}\xi_1 + \delta\eta_1$. Then $S_1 \equiv L_{1,-\delta\beta_{11}^{-1}} S'$ replaces η_1 by $\beta_{11}\xi_1$. For S_1,

$$\gamma_{11} = -\beta_{11}^{-1}, \qquad \gamma_{21} = 0, \qquad \delta_{21} = 0, \qquad \alpha_{22}\delta_{22} - \beta_{22}\gamma_{22} = 1,$$

by certain abelian conditions. Then $S_2 \equiv S_1 U^{-1}$, U as above, is

$$\xi_1' = \alpha_{11}\xi_1 - \beta_{11}^{-1}\eta_1 + \alpha_{12}\xi_2 + \gamma_{12}\eta_2, \qquad \eta_1' = \beta_{11}\xi_1, \qquad \xi_2' = \xi_2 + \alpha_{21}\xi_1,$$
$$\eta_2' = \eta_2 + \beta_{21}\xi_1.$$

Then $S_3 \equiv S_2 N_{1,2,-\gamma_{12}} Q_{1,2,-\alpha_{12}}$ is of the form

$$\xi_1' = \alpha\xi_1 - \beta_{11}^{-1}\eta_1, \qquad \eta_1' = \beta_{11}\xi_1, \qquad \xi_2' = \xi_2, \qquad \eta_2' = \eta_2.$$

Then $S_4 \equiv S_3 L_{1,-\alpha\beta_{11}^{-1}}$ is of the form S_3 with $\alpha = 0$. Now S_4 transforms $L_{1,\lambda}$ into $L'_{1,-\lambda\beta_{11}^2}$. Hence we reach every $L'_{1,\rho}$ and hence $M_1 = L'_{1,-1} L_{1,1} L'_{1,-1}$.

3. THEOREM. *If a subgroup of $SA(4, p^n)$ contains $H_{\omega'}$, it lies in H_ω. In particular, H_ω is a maximal subgroup.*

I omit the proof, which is of the same character as that of § 2.

4. THEOREM. *If, for $p > 2$, a subgroup of $SA(4, p^n)$ contains $K_{\pi'}$, it lies in K_π or G_ω. In particular, K_π is a maximal subgroup.**

We extend $K_{\pi'}$ by a transformation S of $SA(4, p^n)$, lying in neither K_π nor G_ω, and prove that the group obtained is $SA(4, p^n)$. Giving S the notation (1) of $\mathrm{II}_{3\gamma 2}$, we have $\alpha_{12}, \gamma_{12}, \beta_{12}, \delta_{12}$ not all zero, since S does not lie in K_π.

Applying $L_{1,\lambda}$ on the right, we may suppose that α_{12} and γ_{12} are not both zero. We may take $\alpha_{12} \neq 0$, applying M_2 on the left if necessary. Finally, applying $T_{2,\rho} L_{2,\sigma}$ on the left, we may take $\alpha_{12} = 1$, $\gamma_{12} = 0$.

Case (a). Let $\delta_{12} = 0$. Then $(2)_2$ holds. Then SU^{-1}, where $U = \left(\begin{smallmatrix} \alpha_{22} & \gamma_{22} \\ \beta_{22} & \delta_{22} \end{smallmatrix}\right)$ on ξ_2 and η_2, becomes S_1 in view of abelian conditions C_{14}, C_{24}:

$$(5) \qquad S_1 = \begin{bmatrix} \alpha_{11} & \gamma_{11} & 1 & 0 \\ \beta_{11} & \delta_{11} & \beta_{12} & 0 \\ 0 & 0 & 1 & 0 \\ \beta_{21} & \delta_{21} & 0 & 1 \end{bmatrix}, \qquad W = \begin{bmatrix} \alpha & \gamma & 0 & 0 \\ \beta & \delta & 1 & 0 \\ 0 & 0 & 1 & 0 \\ \alpha & \gamma & 0 & 1 \end{bmatrix}.$$

Since S_1 does not lie in G_ω, β_{11} and β_{12} are not both zero.

Let first $\beta_{12} \neq 0$ in S_1. Then $T_{2,\beta_{12}}^{-1} S_1 L_{1,-\beta_{12}^{-1}} T_{2,\beta_{12}}$ is the form W. Then for any $\lambda \neq 0$, $W^{-1} T_{2,\lambda} W T_{2,\lambda}^{-1} = R_{1,2,1-\lambda}$. Transforming by $T_{2,\rho}$ and M_2^{-1}, we reach every $R_{1,2,\mu}$ and $Q_{2,1,\mu}$, if $p^n > 2$. Then† we reach $N_{1,2,\mu}$ and its

* The latter is true also for $p = 2$.

†*Linear Groups*, p. 97, formula (83) for $i = 2, j = 1$.

transform $Q_{1,2,-\mu}$ by M_2. Applying (4), we obtain the remaining generators of $SA(4, p^n)$.

Let next $\beta_{12}=0$, $\beta_{11}\neq 0$, in S_1. Then $\beta_{21}=-\beta_{11}$, $\delta_{21}=-\delta_{11}$ by abelian conditions C_{13} and C_{23}. Then $L_{1,-\delta_{11}\beta_{11}^{-1}} S_1 L_{1,-\alpha_{11}\beta_{11}^{-1}}$ is Z:

$$(6)\quad Z=\begin{bmatrix} 0 & -\beta_{11}^{-1} & 1 & 0 \\ \beta_{11} & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -\beta_{11} & 0 & 0 & 1 \end{bmatrix}, \qquad V=\begin{bmatrix} \alpha_{11} & \gamma_{11} & 1 & 0 \\ \beta_{11} & \delta_{11} & 0 & \delta_{12} \\ \alpha_{21} & \gamma_{21} & 1 & 0 \\ -\beta_{11} & -\delta_{11} & 0 & \delta_{22} \end{bmatrix}$$

$$(\delta_{12}\neq 0,\ \delta_{12}+\delta_{22}=1.)$$

Then if $\gamma\neq 0$, $Z^{-1}T_{2,\lambda}ZT_{2,\lambda}^{-1}=Q_{1,2,\lambda-1}$. If $p>2$, we reach every $Q_{1,2,\tau}$. Then

$$ZQ_{1,2,-1}\colon\ \xi_1'=-\beta_{11}^{-1}\eta_1,\ \eta_1'=\beta_{11}\xi_1,\ \xi_2'=\xi_2,\ \eta_2'=\eta_2$$

transforms $L_{1,\rho}$ into $L'_{1,-\rho\beta_{11}^2}$. We thus reach every transformation of determinant unity on ξ_1 and η_1, and then $SA(4, p^n)$.

Case (b). Let next $\delta_{12}\neq 0$. Applying $L'_{2,\rho}$ on the left we may make $\beta_{12}=0$. We thus have a transformation S' with $\alpha_{12}=1$, $\gamma_{12}=0$, $\beta_{12}=0$, $\delta_{12}\neq 0$. Since S' is not in K_π, α_{22}, γ_{22}, β_{22}, δ_{22} are not all zero. Applying M_2 on the right, we may assume that α_{22} and γ_{22} are not both zero in S'.

(b_1). Let first $\alpha_{22}\neq 0$. We may set $\alpha_{22}=1$ by multiplying by $T_{2,\alpha_{22}}^{-1}$ on the right. Then $V=L_{2,-\gamma_{22}}S'L_{1,\gamma_{22}\delta_{12}^{-1}}L'_{2,-\beta_{22}}$ is of the form $(6)_2$.

If $\alpha_{21}\neq 0$ in V, then $V_1=L_{1,-\gamma_{21}\alpha_{21}^{-1}}V$ has $\gamma_{21}=0$, $\gamma_{11}=0$. Then $V_1^{-1}L'_{2,-\rho}V_1L'_{2,\rho}$ is Z_t, with $t=\rho-\rho\delta_{22}^2$:

$$(7)\quad Z_t=\begin{bmatrix} 1 & 0 & 0 & 0 \\ -\rho\delta_{12}^2 & 1 & -\rho\delta_{12}\delta_{22} & 0 \\ 0 & 0 & 1 & 0 \\ -\rho\delta_{12}\delta_{22} & 0 & t & 1 \end{bmatrix}, \qquad X=\begin{bmatrix} \alpha & \gamma & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & \gamma \\ 0 & 1 & 0 & -\alpha \end{bmatrix}.$$

Then $Z_tL'_{2,-t}=Z_0$. For $\delta_{22}\neq 0$, Z_0 with $\rho=-\delta_{12}^{-1}\delta_{22}^{-1}$ is of the earlier type $(5)_2$. For $\delta_{22}=0$, $Z_0=L'_{1,-\rho}$ and $\delta_{12}=1$, $\alpha_{11}=0$, $\delta_{11}=-\alpha_{21}^{-1}$ in V_1. Then

$$V_2\equiv L'_{1,\beta_{11}\alpha}V_1T_{2,\alpha^{-1}}\colon\ \xi_1'=\xi_2,\ \eta_1'=\eta_2-\alpha^{-1}\eta_1,\ \xi_2'=\xi_1+\alpha^{-1}\xi_2,\ \eta_2'=\eta_1.$$

Then $(V_2^{-1}T_{2,-1}V_2T_{2,-1})^2=Q_{2,1,-4\alpha^{-1}}$. We thus reach $SA(4, p^n)$.

If $\alpha_{21}=0$ in V, then $\alpha_{11}=0$ by abelian condition C_{14}. Applying $L_{1,\rho}$ on the left, we may set $\delta_{11}=0$. Then $L_{2,-\delta_{11}}VL_{1,\delta_{22}\delta_{21}^{-1}}L_{2,1}$ is of the form $(6)_2$ with $\alpha'_{21}=-\beta_{11}\neq 0$.

(b_2). Let finally $\alpha_{22}=0$, $\gamma_{22}\neq 0$ in S'. We may set $\beta_{22}=0$, since otherwise $S'L_{2,1}$ is of the form S' with $\alpha_{22}\neq 0$. Applying on the right the inverse

of $\left(\begin{smallmatrix}\alpha_{21} & \gamma_{21}\\ \beta_{21} & \delta_{21}\end{smallmatrix}\right)$ on ξ_2 and η_2, we reach $(7)_2$, in view of the abelian conditions. If $\alpha=\gamma=0$, $X=P_{12}$ would belong to K_π. If $\alpha\neq 0$, X^{-1} is of the form S' with $\alpha_{22}\neq 0$. Hence we may set $\alpha=0$, $\gamma\neq 0$. Then $X^2=N_{1,2,2\gamma}$. If $p>2$, we reach every $N_{1,2,\rho}$. Now $XN_{1,2,-\gamma}=P_{12}$. Hence we reach the generators of $SA(4,p^n)$.

The subgroups of order a power of p.

5. Consider the subgroup $G_{p^{4n}}$ of the operators $S=[k,a,c,d]$ defined by (3) of II_{372}. Let $\Sigma=[\kappa,\alpha,\gamma,\delta]$. Then the commutator $S^{-1}\Sigma^{-1}S\Sigma$ is

$$[k',0,c',0] \quad (k'=2\alpha c-2\gamma a+\alpha^2 d-a^2\delta,\ c'=\alpha d-a\delta). \tag{8}$$

If $p>2$, we may make k' and c' assume arbitrary values in the field by taking $a=-1$, $\alpha=0$, $\delta=c'$, $2\gamma=k'+c'$. If $p=2$, we may make k' and c' assume arbitrary values each $\neq 0$ by taking $\delta=0$, $\alpha=k'/c'$, $d=c'^2/k'$; also we may make $k'=c'=0$. The number of operators thus reached is $(2^n-1)^2+1$, which exceeds $\frac{1}{2}2^{2n}$ if $n>1$, so that they generate $K_{2^{2n}}$ below. If $p=2$, $n=1$, then $k'=c'=\alpha d-a\delta$.

THEOREM. *For $p^n>2$, the commutator subgroup of $G_{p^{4n}}$ is*

$$K_{p^{2n}}=\{[k,0,c,0],\ k,c \text{ arbitrary}\}; \tag{9}$$

for $p^n=2$ it is the group of the two operators $[k,0,k,0]$, $k=0,1$.

6. It is easily shown that if the pth power of every operator of a group G_{p^a} belongs to its commutator subgroup G_{p^b}, there are exactly $(p^{a-b}-1)/(p-1)$ subgroups of order p^{a-1} in G_{p^a}.

For $G_{p^{4n}}$ the condition is satisfied. Hence the number of its subgroups of order p^{4n-1} is $(p^{2n}-1)/(p-1)$ if $p^n>2$, and 7 if $p^n=2$.

When a subgroup $G_{p^{4n}}$ can be defined by certain independent relations $f_1=0,\cdots,f_r=0$ between the coefficients k,a,c,d of S, we denote it $\{f_1=0,\cdots,f_r=0\}$. Thus (9) is denoted $\{a=0,d=0\}$.

For $p>2$, $n=1$, the $p+1$ subgroups of order p^3 of G_{p^4} are

$$\{d=0\}, \qquad \{a=td\} \qquad (t=0,1,\cdots,p-1). \tag{10}$$

7. The group $\{a=0\}$ is commutative of type $(1,1,1)$ and hence has p^2+p+1 subgroups of order p^2. As in §5, it follows that, for $p>2$, the commutator group of either $\{d=0\}$ or $\{a=td\}$, $t\neq 0$, is formed of the operators $[k,0,0,0]$, and contains the pth power of every S. Hence either group has exactly $p+1$ subgroups of order p^2. They are seen to be the ones given in the following table:

Order p^3.	Subgroups of order p^2.
$\{d=0\}$	$\{d=0, a=0\}$, $\{d=0, c=sa\}$,
$\{a=td\}$, $t\neq 0$	$\{a=0, d=0\}$, $\{a=td, c=sd+\frac{1}{2}td^2\}$,
$\{a=0\}$	$\{a=0, d=0\}$, $\{a=0, c=sd\}$, $\{a=0, k=rc+sd\}$

where r and s take independently the values $0, 1, \cdots, p-1$.

Now $T_{1,t^{-1}}$ transforms $\{a=td\}$, $t\neq 0$, into $\{a=d\}$. The $2p^2+p+1$ distinct subgroups of order p^2 of G_{p^4} are found to be conjugate within $SA(4,p)$ with the four types* in the 5th–8th rows of the table of §8.

8. In the following table is given in the first column a representative of each set of subgroups of G_{p^4} conjugate within $SA(4,p)$, $p>2$; in the second column the largest subgroup of $SA(4,p)$ transforming into itself the representative.

G_{p^4}	G_{p^4}, $T_{1,a_{11}}T_{,a_{22}}$
$\{a=0\}$	H_ω of operators $(1)_2$
$\{d=0\}$	G_ω of operators $(1)_1$
$\{a=d\}$	G_{p^4}, $T_{1,a^3}T_{2,a}$
$\{a=d=0\}$	G_{p^4}, $T_{1,a_{11}}T_{2,a_{22}}$
$\{a=c=0\}$	$\{a=0\}$, $T_{1,a_{11}}T_{2,a_{22}}$, P_{12}
$\{a=0, k=\nu d\}$	$2p^3(p^2-1)$ operators $(11)_1$
$\{a=d, c=\frac{1}{2}d^2\}$	$\{a=d\}$, $T_{1,a^3}T_{2,a}$
(L_{11})	G_ω of operators $(1)_1$
$(L_{1\mu}L_{21})$	$(p\mp\epsilon)(p-1)p^3$ operators $(11)_2$
(B) if $p>3$	$\left[\gamma, \alpha, \frac{\alpha+\alpha^2}{2}, \alpha\right]$, $T_{1,s^3}T_{2,s}\left[0, 0, \frac{s^4-1}{12}, \frac{s^2-1}{2}\right]$

where ν is a particular not-square, $\mu=1$ or ν, $B=[0,-1,0,-1]$, and $\epsilon=\pm 1$ according as $p=4l\pm 1$, and where

$$(11)\quad \begin{Vmatrix} \pm\alpha_{22} & \gamma_{11} & \pm\nu\alpha_{21} & \gamma_{12} \\ 0 & \alpha_{22}/\Delta & 0 & -\alpha_{21}/\Delta \\ \alpha_{21} & \gamma_{21} & \alpha_{22} & \gamma_{22} \\ 0 & \mp\nu\alpha_{21}/\Delta & 0 & \pm\alpha_{22}/\Delta \end{Vmatrix}, \quad \begin{Vmatrix} \alpha_{11} & \gamma_{11} & \alpha_{12} & \gamma_{12} \\ 0 & t^{-1}\alpha_{11} & 0 & t^{-1}\mu^{-1}\alpha_{12} \\ \mp\mu^{-1}\alpha_{12} & \gamma_{21} & \pm\alpha_{11} & \gamma_{22} \\ 0 & \mp t^{-1}\alpha_{12} & 0 & \pm t^{-1}\alpha_{11} \end{Vmatrix}$$

$$\Delta=\pm(\alpha_{22}^2-\nu\alpha_{21}^2)\neq 0,\quad t=\alpha_{11}^2+\mu^{-1}\alpha_{12}^2\neq 0.$$

* These correspond to K_{p^3}, $K_{p^2}^{*}$, $K_{p^2}^{**}$, and $(16')$, respectively of II. The types of period p are taken from I; the transform of A_1 of I_{112} by $M_1M_2T_{1,-1}$ gives B.

General plan of the subsequent investigation.

9. Let H be a subgroup of order p^iN of $SA(4, p)$, $i > 0$, N prime to p, $p > 2$. Applying a suitable transformation within $SA(4, p)$, we may assume that H contains a subgroup G_{p^i} lying in the G_{p^4} of §§ 5–7. If H contains G_{p^i} self-conjugately, H lies in one of the groups in the second column of the table in § 8, and hence lies in G_ω, H_ω, or $(G_{p^4}, T_{1, a_{11}} T_{2, a_{22}})$. In this case the determination of H depends upon the determination* of all subgroups of the binary linear-homogeneous group of determinant unity. Suppose next that G_{p^i} is not self-conjugate in H. Let p^m be the maximal order of a subgroup common to G_{p^i} and any of its conjugates under H; let G_{p^m} be such a subgroup. By a theorem† discovered independently by BURNSIDE and FROBENIUS, H must contain an operator S, of period prime to p, commutative with G_{p^m} but not with G_{p^i}.

Now, if $p > 2$, $(p^4 - 1)(p^2 - 1)$ has no factor of the form $1 + p^3x$, $x > 0$. For if so, call the quotient q. Then $0 < q < p^3$, $-p^2 + 1 \equiv q \pmod{p^3}$. Hence $q = p^3 - p^2 + 1$. But the latter is relatively prime to $(p^2 - 1)^2$, and exceeds $p^2 + 1$ if $p > 2$. Hence the number of conjugates to G_{p^i} in H is not $\equiv 1 \pmod{p^3}$, so that‡ $m \geqq i - 2$. *We may set* $m = i - 1$ *or* $i - 2$.

10. LEMMA. *Any binary transformation* $B = \left(\begin{smallmatrix} \alpha & \gamma \\ \beta & \delta \end{smallmatrix}\right)$, $\beta \neq 0$, *together with all the* $S_\lambda = \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$ *generate every binary transformation of determinant unity.*

Indeed, $S_{-\delta\beta^{-1}} B S_{-\alpha\beta^{-1}} = \left(\begin{smallmatrix} 0 & \tau \\ \beta & 0 \end{smallmatrix}\right)$, where $\tau = -\beta^{-1}(\alpha\delta - \beta\gamma) \neq 0$. The latter operator transforms S_λ into $\left(\begin{smallmatrix} 1 & 0 \\ \sigma & 1 \end{smallmatrix}\right)$, where $\sigma = \lambda\beta\tau^{-1}$ may be made arbitrary.

The subgroups H of order p^4N, $p > 2$.

11. Now $i = 4$, $m = 3$ or 2 in § 9. For $m = 3$, we may take G_{p^m} to be $\{a = 0\}$ or $\{d = 0\}$, since every operator commutative with $\{a = d\}$ lies in $(G_{p^4}, T_{1a^2} T_{2, a})$ and hence is commutative with G_{p^4} (§ 8).

For $\{d = 0\}$, S is of the form $(1)_1$. Then $\beta_{22} \neq 0$ since S is not commutative with G_{p^4}. The quotient-group§ $G_\omega / \{d = 0\}$ may be taken concretely as the group of the products $T_{1, a_{11}} U$, U a binary transformation of determinant unity on ξ_2 and η_2. Also, $G_{p^4} / \{d = 0\}$ is $(L_{2, \gamma})$. Then, by § 10, we reach every U. These, with G_{p^4}, generate $G_{\omega'}$. Hence, by § 2, H is a subgroup of G_ω.

For $\{a = 0\}$, S is of the form $(1)_2$, with $\alpha_{21} \neq 0$. The quotient-groups

* This has been done by the writer for any Galois field.

† References in BURNSIDE's *Theory of Groups*, p. 97.

‡ Compare, for example, BURNSIDE's *Theory of Groups*, p. 94, Cor. II.

§ Bulletin of the American Mathematical Society, vol. 10 (1904), pp. 178–184.

$$\frac{H_\omega}{\{a=0\}} = \begin{bmatrix} \alpha_{11} & 0 & \alpha_{12} & 0 \\ 0 & \alpha_{22}/\Delta & 0 & -\alpha_{21}/\Delta \\ \alpha_{21} & 0 & \alpha_{22} & 0 \\ 0 & -\alpha_{12}/\Delta & 0 & \alpha_{11}/\Delta \end{bmatrix}, \qquad \frac{G_{p^4}}{\{a=0\}} = \begin{bmatrix} 1 & 0 & a & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -a & 0 & 1 \end{bmatrix},$$

where $\Delta = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}$, are simply isomorphic with the binary groups

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}, \qquad \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

Hence, in view of § 10 and § 3, H is a subgroup of H_ω.

12. Let next $i=4$, $m=2$. Then, by § 8, G_{p^2} is neither $\{a=d=0\}$ nor $\{a=d,\ c=\frac{1}{2}d^2\}$. If G_{p^2} is $\{a=c=0\}$, $S=S_1P_{12}$, where S_1 lies in $\{a=0\}$ extended by T_{1,a_1}, T_{2,a_2}, so that S_1 transforms G_{p^4} into itself. But G_{p^4} and its transform by P_{12} have $\{a=0\}$ in common, in contradiction with $m=2$. Finally, let G_{p^2} be $\{a=0,\ k=\nu d\}$, so that S is of the form $(11)_1$. Now the general quaternary abelian operator with every $\beta_{ij}=0$ transforms $[k, a, c, d]$ into an operator of the form $(1)_2$, written in capital letters, with

$$A_{ij} = \tau_{ij} + a\alpha_{i1}\delta_{j2}, \qquad D_{ij} = \tau_{ij} - a\delta_{i2}\alpha_{j1},$$
$$C_{ij} = k\alpha_{i1}\alpha_{j1} + c\alpha_{i1}\alpha_{j2} + (c-ad)\alpha_{i2}\alpha_{j1} + d\alpha_{i2}\alpha_{j2} - a\alpha_{i1}\gamma_{j2} - a\gamma_{i2}\alpha_{j1},$$

where $\tau_{ij}=1$ $(i=j)$, $\tau_{ij}=0$ $(i\neq j)$. Hence G_{p^4} and its transform by S would have $\{a=0\}$ in common, in contradiction with $m=2$.

The subgroups H of order p^3N, $p>2$.

13. Let first $i=3$, $m=2$ in § 9. In view of § 8 the only case not immediately excluded is $G_{p^2}=\{a=d=0\}$, $G_{p^3}=\{a=d\}$. Then S lies in $(G_{p^4}, T_{1,a_{11}}T_{2,a_{22}})$ and hence transforms $\{a=d\}$ into $\{a=\alpha_{11}\alpha_{22}^{-3}d\}$; the latter two generate G_{p^4} in contradiction with $i=3$.

14. Let $i=3$, $m=1$. If $G_p=(L_{1,\mu}L_{2,1})$, then $G_{p^3}=\{a=0\}$. Since $(11)_2$ is of the form $(1)_2$, this case is excluded by § 8. If $G_p=(B)$, p being >3, then $G_{p^3}=\{a=d\}$; so that (§ 8) any operator commutative with G_p is commutative with G_{p^3}. Let finally $G_p=(L_{1,1})$. Let first G_{p^3} be $\{a=0\}$, so that S is of the form $(1)_1$ with $\beta_{22}\neq 0$. Then S transforms $[0,0,1,0]$ into $[2\alpha_{11}\alpha_{12}, -\alpha_{11}\beta_{22}, \alpha_{11}\alpha_{22}, 0]$, which extends G_{p^3} to G_{p^4}, in contradiction with $i=3$. The same argument excludes $G_{p^3}=\{a=d\}$. Finally, $G_{p^3}=\{d=0\}$ is excluded by § 8.

THEOREM. *Every subgroup of order p^3N has a self-conjugate G_{p^3} and hence lies in either G_ω or H_ω.*

The subgroups H of order p^2N, $p>2$.

15. Let $i=2$, $m=1$. Let first $G_p=(L_{1,1})$, whence $S=(1)_1$. Then G_{p^2} is

$$\{a=d=0\}, \qquad \{a=c=0\}, \qquad \text{or} \qquad \{a=d,\ c=sd+\tfrac{1}{2}d^2\}.$$

We may set $s=0$ by transforming by $[0,0,-s,0]$, which is commutative with $(L_{1,1})$. The argument at the end of § 14 excludes $\{a=d=0\}$.

Let $G_{p^2}=\{a=c=0\}$. Now S transforms $[k,0,0,\gamma]$ into Σ, given by the second matrix of $\Pi_{37.4}$ when $a=c=0$. The supposition $\beta_{22}=0$ contradicts $i=2$. If $\alpha_{22}\neq 0$, we employ Σ for $\gamma=\alpha_{22}^{-1}\beta_{22}^{-1}$. Hence we may set $\beta_{22}\neq 0$, $\alpha_{22}=0$ in S. Then, for $\gamma=-\beta_{22}^{-2}$, $\Sigma L_{1,-k'}$ has the form $L'_{2,1}Q_{1,2,\delta}$. This is transformed into $L'_{2,1}L_{1,\delta^2}$ by $N_{1,2,-\delta}$, which is commutative with $\{a=c=0\}$. Hence H contains $L'_{2,1}$ and $\{a=c=0\}$, which generate $K_{\pi'}$ of § 1. By § 4, H lies in K_π or G_ω.

For $G_{p^2}=\{a=d,\ c=\frac{1}{2}d^2\}$, a similar argument shows H contains an operator $U_{r,s}$, with $s\neq 0$:

$$U_{r,s}=\begin{Bmatrix}1&0&r&s\\0&1&0&0\\0&s-r&1&0\\0&s-r&1&1\end{Bmatrix}, \qquad X=\begin{Bmatrix}1&0&\frac{1}{2}&\frac{1}{2}\\0&1&0&0\\0&-\frac{1}{2}&0&1\\0&-\frac{3}{2}&-1&2\end{Bmatrix}.$$

Now $N_{1,2,-r}$, which is commutative with G_{p^2}, transforms $U_{r,s}$ into $L_{1,r^2-rs}U_{0,s}$. Hence, H contains G_{p^2} and $U_{0,s}$. Set $E_d=[0,d,d^2/2,d]$. Then H contains $X\equiv L_{1,2s}U_{0,s}^{-1}E_1U_{0,s}$, and Y, the transform of E_{-1} by $[2,2,2,2]X$. Now $N_{1,2,2}$ transforms G_{p^2} into itself, and Y into $L_{1,27/4}U_{0,1}$. We may thus assume that H contains G_{p^2} and $U_{0,1}$. Then H contains

$$X^{-1}L_{1,\frac{9}{4}}E_{-1}U_{0,1}^{-1}E_1=[-1,-2,0,0],$$

which belongs to G_{p^3}, but not to G_{p^2}, contrary to $i=2$.

16. Let next $G_p=(L_{1,\mu}L_{2,1})$. Then S is of the form $(11)_2$, a special case of $(1)_2$. Hence S transforms $\{a=0\}$ into itself. But the only G_{p^2} containing G_p are $\{a=c=0\}$ and $\{a=0,\ k=rc+\mu d\}$. Hence S transforms either of these into a subgroup of G_{p^3}, in contradiction with $i=2$.

17. Let finally $G_p=(B)$, p being >3. Then G_{p^2} must be either

$$\{a=d=0\}, \qquad \text{or} \qquad \{a=d,\ c=\sigma d+\tfrac{1}{2}d^2\}.$$

The first is excluded by § 8. The second is transformed into itself by any

operator of $\{a = d\}$, and into $\{a = d, c = s^2\sigma d + \frac{1}{2}d^2\}$ by $T_{1,s^2}T_{2,s}$. Transforming the result by $[0, 0, (s^4-1)/12, (s^2-1)/2]$, we obtain

$$\{a = d, c = [s^2\sigma - \tfrac{1}{2}(s^2-1)]d + \tfrac{1}{2}d^2\}.$$

This lies in G_{p^4}, in contradiction with $i = 2$.

18. It remains to consider the H_{p^2N} no two of whose subgroups G_{p^2} have in common an operator $\neq I$. Hence the number of conjugate G_{p^2} is M, where $M \equiv 1 \pmod{p^2}$. It is readily shown that the only factors of the form $1 + p^2x$ of $\omega = (p^4-1)(p^2-1)$ are $1, p^2+1, (p^2-1)^2$ and ω. Hence if H is of index $< \tau$, where $\tau = (p^4-1)/(p-1)$, we may set $M = p^2+1$ or $(p^2-1)^2$. The latter case is immediately excluded in view of the orders of the largest subgroups containing a G_{p^2} self-conjugately (§ 8). For $M = p^2+1$, G_{p^2} is self-conjugate in a G_{p^2t} within H, where t divides $(p^2-1)^2$. In fact, $t \leqq 2(p^2-1)$ by § 8. Hence, for $p > 3$, H is of index $> \tau$.

19. If a subgroup H of order pN is of index $< \tau$, then $N = \omega$. The details of the exclusion (for $p > 3$) of this isolated case will be omitted, in view of an anticipated treatment of all orders pN. In this direction I have shown that any H_{pN} with more than one C_p conjugate with $(L_{1,1})$ may be transformed into the group Γ of the binary transformations of determinant unity on ξ_1 and η_1, or else into a direct product of Γ and a binary group on ξ_2 and η_2 with no operator of period p (and hence of order $2, 4d, 24, 48$ or 120).

THE UNIVERSITY OF CHICAGO,
October 1, 1904.

DETERMINATION OF ALL THE GROUPS OF ORDER 2^m WHICH CONTAIN AN ODD NUMBER OF CYCLIC SUBGROUPS OF COMPOSITE ORDER*

BY

G. A. MILLER

It has recently been proved that in every non-cyclic group of order p^m, p being an odd prime, the number of cyclic subgroups of order p^β, $\beta > 1$, is always a multiple of p, and that this number is of the form $1 + p + kp^2$ when $\beta = 1$.† From this it follows almost directly that the number of cyclic subgroups of order p^β in any group (G) is always of the form kp whenever the Sylow subgroups of order p^m in G are non-cyclic, and that the number of subgroups of order p in such a G is always of the form $1 + p + kp^2$.‡ When $p = 2$, both of these theorems have exceptions. The present paper is devoted to an exhaustive study of the exceptions of the former theorem. Since the cyclic groups are so elementary we shall confine our attention to the non-cyclic groups of order 2^m. Moreover, every group of even order contains an odd

* Presented to the Society (San Francisco) October 1, 1904. Received for publication September 26, 1904.

† Proceedings of the London Mathematical Society, ser. 2, vol. 2 (1904), p. 142.

‡ The former of these facts was noticed in the article just mentioned. The second does not follow so easily, but it may be proved as follows: Since the number of subgroups of order p in such a Sylow subgroup (S) of order p^m is $\equiv 1 + p \pmod{p^2}$, it is only necessary to observe that the number of those which are found in G but not in S is of the form kp^2. If S transforms one of these subgroups (P) into only p conjugates, the operators of P are commutative with every operator of a subgroup of order p^{m-1} contained in S. In particular, P and an invariant (under S) operator of order p in this subgroup of order p^{m-1} generate a group of order p^2 and of type $(1, 1)$ which has just p conjugates under S. It could not be transformed into itself by S since a Sylow subgroup cannot transform a group of order p^γ into itself unless this group is contained in the Sylow subgroup. The given p subgroups of order p^2 contain p^2 distinct subgroups of order p which are not found in S and whose generators are commutative with each operator of the given subgroup of order p^{m-1}. If there is any other operator (P) of order p in G which is not found in S and is commutative with each operator of the given subgroup of order p^{m-1}, we use the same invariant operator under S and construct other p conjugate subgroups under S which have p^2 additional subgroups of order p, etc. Proceeding in the same manner with each of the other subgroups of order p^{m-1} in S, the theorem clearly follows since we do not need to consider those subgroups of order p which have more than p conjugates under S. When the Sylow subgroups of order p^m $(p > 2, m > 1)$ in G are cyclic, the preceding argument proves that the number of subgroups of order p is of the form $1 + kp^2$.

number of subgroups of order 2 since the operators of order 2 and the identity are the only ones which are self inverse.

§ 1. *Cyclic subgroups whose order exceeds four.*

We shall first prove that a group of order 2^m cannot contain just $2n+1$, $n>0$, cyclic subgroups of order 2^α, $\alpha>2$. Suppose that such a group (G) contains $2n+1$ cyclic subgroups of order 2^α. At least one of them (H_1) is invariant under G. Let H_2 represent any other and let H_2' be the subgroup of H_2 such that the group $\{H_1, H_2'\}$ generated by H_1, H_2' is of order $2^{\alpha+1}$. When H_2' coincides with H_2 then $\{H_1, H_2'\}$ contains just 2 cyclic subgroups of order 2^α.* If this condition is not satisfied H_2' must transform H_1 according to the square of an operator in its group of isomorphism. Hence $\{H_1, H_2'\}$ has still just 2 cyclic subgroups of order 2^α and at least $2^{\alpha-1}$ invariant operators.† These two cyclic subgroups, which we may call H_1, H_2, contain just $2^{\alpha-1}$ common operators. It will next be proved that G contains an even number of cyclic subgroups of order 2^α which involve these $2^{\alpha-1}$ common operators. The main result thus far is that any group which contains an odd number (greater than one) of cyclic subgroups of order 2^α must contain two such subgroups which have $2^{\alpha-1}$ common operators.

Suppose that G contains an odd number of cyclic subgroups of order 2^α which have $2^{\alpha-1}$ operators in common with H_1. One of them (H_3) must be transformed into itself by $\{H_1, H_2\}$. The group $\{H_1, H_2, H_3\}$ is clearly conformal to an abelian group with respect to its operators whose orders exceed 4. This follows almost directly from the fact that the order of the commutator subgroup of this group cannot exceed 2. Hence $\{H_1, H_2, H_3\}$ contains four cyclic subgroups of order 2^α. At least one of the remaining cyclic subgroups of order 2^α which have $2^{\alpha-1}$ operators in common with H_1 is transformed into itself by $\{H_1, H_2, H_3\}$. Calling this H_5 we have again that the group $\{H_1, H_2, H_3, H_5\}$ is conformal with an abelian group with respect to its operators whose order exceed four. This group contains 8 cyclic subgroups of order 2^α. As this process could be continued indefinitely if there were an odd number of cyclic subgroups of order 2^α having $2^{\alpha-1}$ operators in common with H_1, this hypothesis is disproved.

The theorem in question is now practically proved, for the cyclic subgroups of order 2^α which have $2^{\alpha-1}$ common operators must occur in even sets and a cyclic group of order 2^α which is found in one set cannot also occur in another set. Hence *G cannot contain just $2n+1$, $n>0$, cyclic subgroups of order 2^α, $\alpha>2$.* We shall now consider the case when G contains only one cyclic

* BURNSIDE, *Theory of Groups of Finite Order*, 1897, p. 77.

† Bulletin of the American Mathematical Society, vol. 7 (1901), p. 352.

subgroup of order 2^α. It will result that in this case G must be one of these three well known groups of order $2^\alpha + 1$ having this property; viz., the dihedral rotation group, the one obtained from this dihedral rotation group by replacing its non-invariant operators of order 2 by operators of order 4, and the one which transforms the operators of the cyclic subgroup of order 2^{α_1} into their $2^{\alpha_1} - 1$ powers, containing $2^{\alpha_1} - 1$ operators of each of the orders 2 and 4 in addition to the given cyclic subgroup.

If G contains only one cyclic subgroup of order 2^α it cannot contain more than one cyclic subgroup of any higher order (2^{α_1}), since some two subgroups of this order would generate a group which is conformal with the abelian group of the type $(\alpha_1, 1)$.* Let 2^{α_1} be the order of the largest cyclic subgroup H_1 of G. The operators of G must transform the operators of H_1 according to a group of order $2^{m-\alpha_1}$. Every subgroup of order 4 in the group of isomorphisms of H_1 contains the operator of order 2 which transforms just half of the operators of H_1 into themselves.† Hence $m = \alpha_1 + 1$, otherwise G would contain more than one cyclic subgroup of order 2^{α_1} as it would have to transform the operators of H_1 according to the given operator of order 2. As the groups of order $2^{\alpha_1} + 1$ which contain a cyclic subgroup of order 2^{α_1} are well known, the results stated at the end of the preceding paragraph are established. That is, *if a group of order 2^m contains an odd number of cyclic subgroups of order 2^α, $\alpha > 2$, this number must be unity, and the group must be one of three containing a cyclic subgroup of order 2^{m-1}.* As the properties of these three groups are very elementary and their forms are so dissimilar (one contains $2^{m-1} + 1$, the other $2^{m-2} + 1$, and the third only one operator of order 2) it is easy to distinguish them. When α is given, m may have any arbitrary value which exceeds α.

§ 2. *Cyclic subgroups of order four.*

The three groups mentioned in the last paragraph contain respectively one, $2^{m-3} + 1$, and $2^{m-2} + 1$ cyclic subgroups of order 4. We proceed to prove that these are the only non-cyclic groups of order 2^m which contain an odd number of cyclic subgroups of order 4. The method of proof is very similar to the one employed in the preceding section.

Let G be any group of order 2^m which contains an odd number of cyclic subgroups of order 4. At least one of them (K_1) is invariant under G. At least half the operators of G are commutative with a generator (s) of K_1. It will be proved that the subgroup (G_1) formed by these 2^{m-1} operators must be cyclic. If G_1 were not cyclic K_1 would be contained in an abelian subgroup of

* American Journal of Mathematics, vol. 23 (1901), p. 173.

† Bulletin of the American Mathematical Society, vol. 7 (1901), p. 351.

type $(2, 1)$.* This subgroup would contain two cyclic subgroups of order 4, (K_1, K_2) having a common square. It will now be proved that G would then contain an even number of cyclic subgroups of order 4 including s^2.

If this number were odd, $\{K_1, K_2\}$ would transform at least one of the remaining ones (K_3) into itself. The commutator subgroup of $[K_1, K_2, K_3]$ is generated by s^2 and hence this group contains an even number of cyclic subgroups of order 4 and all of these subgroups contain s^2.† Hence there would be another invariant cyclic subgroup K_4 involving s^2. The number of cyclic subgroups of order 4 in $\{K_1, K_2, K_3, K_4\}$ is again even since the commutator subgroup is still generated by s^2, and all of these subgroups include s^2. This follows almost directly from the fact that the product of an operator of order 4 in $\{K_1, K_2, K_3, K_4\}$ into an operator of order 2 is of order 4 when the two factors are commutative and of order 2 when they are not commutative, while the converse is true when the second factor is of order 4.

As this process could be continued indefinitely if there were an odd number of cyclic subgroups of order 4 which contained s^2, it results that the number of these subgroups is even. If there were an odd numbers of cyclic subgroups of order 4 in G which did not contain s^2, one of these and s^2 would again generate the abelian group of type (2, 1) and the number of those involving the same subgroup of order 2 would again be even. As similar remarks would apply to all the possible other cyclic subgroups of order 4 we have proved that G_1 *is cyclic whenever* G *contains an odd number of cyclic subgroups of order* 4. This proves the statement in the first paragraph of this section, since the other non-cyclic group of order 2^m which contains a cyclic subgroup of order 2^{m-1} contains an even number of cyclic subgroups of order 4.

Combining the results of the two sections we have that every group of order 2^m, $m > 3$, which contains an odd number of cyclic subgroups of order 4 contains just one cyclic subgroup of order 2^α, where α can have all the values from 3 to $m - 1$; and every group which contains only one cyclic subgroup of order 2^α contains an odd number of cyclic subgroups of order 4. For each value of α and m there are three such groups, hence there is a doubly infinite system of groups of order 2^m which contain an odd number of cyclic subgroups of composite order. When $m = 3$ there are only two groups having this property, viz. the quaternion group and the group of movements of the square. If all the non-cyclic groups of order $p^m (m > 3, p$ an arbitrary prime) were determined there would be just three among them in which the number of cyclic subgroups of composite order would not always be a multiple of p. In these three special cases the number of cyclic subgroups of every composite order is not divisible by p.

* BURNSIDE, loc. cit., p. 75.

† Quarterly Journal of Mathematics, vol. 28 (1896), p. 269.

In the exceptional groups noted above the number of the subgroups of order 2 is $\equiv 1 \pmod 4$. That this number is $\equiv 3 \pmod 4$ in every other non-cyclic group of order 2^m is a direct consequence of the fact that the number of cyclic subgroups of order 4 in all of these groups is even. From this fact it results that the number of operators whose order exceeds 2 is divisible by 4, since every cyclic subgroup of order 2^σ contains $2^{\sigma-1}$ operators which are not found in any other subgroup whose order $\leqq 2^\sigma$. Hence the given system of groups is composed of all the groups of order p^m in which the number of cyclic subgroups of order p is not $\equiv 1 + p \pmod{p^2}$. That is, the groups of order p^m in which the number of cyclic subgroups of composite order is not divisible by p coincide with those in which the number of subgroups of order p is not of the form $1 + p + kp^2$.

ON THE COEFFICIENTS IN THE QUOTIENT OF TWO ALTERNANTS*

BY

E. D. ROE, JR.

§ 1. *Introduction.*

This paper is complementary to one published in an earlier number of the Transactions.† The notations used there are retained with the following additions:

$$(1)\qquad \left|\begin{matrix} p_1 p_2 \cdots p_m \\ \kappa_1 \kappa_2 \cdots \kappa_m \end{matrix}\right| = \left|\left[\begin{matrix} p_1 p_2 \cdots p_m \\ q_1 q_2 \cdots q_m \end{matrix}\right]\right| = \left|\left[\begin{matrix} p \\ q \end{matrix}\right]\right|,$$

$$\left|\begin{matrix} \kappa_1 \kappa_2 \cdots \kappa_m \\ (1)^{j_1}(1^2)^{j_2}\cdots(1^n)^{j_n} \end{matrix}\right| = \left[\begin{matrix} q \\ (1^i)^j \end{matrix}\right],$$

where $q_1 = \kappa_1, q_2 = \kappa_2 - 1, \cdots, q_m = \kappa_m - m + 1$, so that p and q are both partitions of weight w;

$$(2)\quad \delta_r f(p_1, p_2, \cdots, p_m) = \Sigma f(p_1 - 1, p_2 - 1, \cdots, p_r - 1, p_{r+1} \cdots p_m),$$

$$(3)\quad \overline{\delta}_r f(p_1, p_2, \cdots, p_m) = \Sigma f(p_1 - r_1, p_2 - r_2, \cdots, p_\lambda - r_\lambda, p_{\lambda+1} \cdots p_m),$$

where

$$r_1 + r_2 + \cdots + r_\lambda = r, \qquad 1 \leqq \lambda \leqq r, \qquad 0 \leqq p_1 - r_1 \leqq p_2 - r_2 \leqq \cdots,$$

and where such terms in Σ are excepted as would present the subtraction of the same number from two or more equal p's;

$$(4)\quad \partial_r f(p_1, p_2, \cdots, p_m) = \partial_r f(1^{x_1} 2^{x_2} \cdots r^{x_r} \cdots m^{x_m}) = f(1^{x_1} 2^{x_2} \cdots r^{x_r - 1} \cdots m^{x_m});$$

$$(5)\quad \partial_r f[(1)^{x_1}(1^2)^{x_2}\cdots(1^m)^{x_m}] = f[(1)^{x_1}(1^2)^{x_2}\cdots(1^r)^{x_r - 1}\cdots(1^m)^{x_m}].$$

* Presented to the Society December 29, 1902. Received for publication May 9, 1904.

† *On the Coefficients in the Product of an Alternant and a Symmetric Function* vol. 5 (1904), no. 2, pp. 193–213. This paper will be referred to as I.

The subject of investigation is the coefficients $|\left[\begin{smallmatrix} p \\ q \end{smallmatrix}\right]|$ of the symmetric functions (p) in the quotient

$$\frac{|\kappa_1 \kappa_2 \cdots \kappa_m|}{|01 \cdots m|} = \sum \begin{vmatrix} p \\ \kappa \end{vmatrix} (p) = \sum \left|\begin{bmatrix} p \\ q \end{bmatrix}\right| (p). \tag{6}$$

A table of such coefficients for weight w is called a quotient table for weight w.

The following results are obtained: The relations

$$\left|\begin{bmatrix} p \\ q \end{bmatrix}\right| = \frac{\partial_r}{\delta_r} \left|\begin{bmatrix} p \\ q \end{bmatrix}\right|, \qquad \text{and} \qquad \sum_{\kappa} \begin{vmatrix} \kappa \\ p \end{vmatrix} \cdot \begin{vmatrix} q \\ \kappa \end{vmatrix} = \begin{matrix} 0 \\ 1 \end{matrix}$$

according as $\begin{matrix} p \neq q \\ p = q \end{matrix}$, together with other recurrence formulas, are found in § 2. Generalizations for some of the columns of coefficients are brought out in § 3. In § 4, it is shown that: the table is contained in a triangle and fills up the remainder of the square with the product table; none of the coefficients is negative; the diagonal line next to the hypotenuse is skew-symmetrical with the corresponding diagonal of the product table; the hypotenuse consists of ones which the table has in common with the product table; the table possesses the invariant property; the coefficients are the conjugates of those of Dr. Taylor's product table; the last line of the table is proved to be symmetrical with respect to its middle element. In addition to the quotients aimed at, the table also gives the determinants $\{\kappa_1 \kappa_2 \cdots \kappa_m\}_a$, or $\{\kappa_1 \kappa_2 \cdots \kappa_m\}_t$ in terms of monomial symmetric functions, and by means of a two-fold application it gives the values of the elementary products of weight w in terms of monomial symmetric functions (§ 5).

§ 2. *Recurrence Formulas for the* $|\left[\begin{smallmatrix} p \\ q \end{smallmatrix}\right]|$.

1. Dr. Taylor has obtained the following formula,* which has been expressed in the writer's notation, viz.:

$$(1^i)^j_{\kappa} = \frac{\delta_r}{\partial_r} (1^i)^j_{\kappa}, \tag{7}$$

where the upper operator δ_r applies to the upper complex only, and the lower one ∂_r to the lower, and where such terms in the summation are excluded as would make two of the κ's equal, since in this case the corresponding alternant would vanish. By using the partition q of weight w, instead of the complex κ, obtained from it as explained in connection with (1), (7) becomes

$$\left[\begin{matrix} q \\ (1^i)^j \end{matrix}\right] = \frac{\delta_r}{\partial_r} \left[\begin{matrix} q \\ (1^i)^j \end{matrix}\right], \tag{8}$$

**On the Product of an Alternant by a Symmetric Function*, American Mathematical Monthly, vol. 10 (1903), pp. 119–130.

where such terms in the sum vanish as cause a smaller number to follow a larger one in the series q.

Example: Using ∂_3, δ_3 as operators, and having the table for weight 4,

$$\left[\begin{matrix}1^2 3\\(1)(1^3)^2\end{matrix}\right]=\left[\begin{matrix}1^2 2\\(1)(1^3)\end{matrix}\right]+\left[\begin{matrix}1^4\\(1)(1^3)\end{matrix}\right]=1+1=2.$$

2. Expressing (7) in terms of conjugates by the relation (30) of I, and by considering the effect on its conjugate of an operator δ_r on a partition, we find that the operator δ_r goes over into its conjugate $\bar{\delta}_r$, whence,

$$\left|\left[\begin{matrix}p\\q\end{matrix}\right]\right|=\frac{\partial_r}{\bar{\delta}_r}\left|\left[\begin{matrix}p\\q\end{matrix}\right]\right|. \tag{9}$$

Formula (9) reduces a coefficient in the quotient table of weight w, to a sum of coefficients in the table of weight $w-r$.

Example: Using ∂_2 and $\bar{\delta}_2$,

$$\left|\left[\begin{matrix}1^3 2^2\\2^2 3\end{matrix}\right]\right|=\left|\left[\begin{matrix}1^3 2\\23\end{matrix}\right]\right|+\left|\left[\begin{matrix}1^3 2\\12^2\end{matrix}\right]\right|=3+2=5,$$

by the table for weight 5.

Since the tables read horizontally give the values of the elementary products in terms of the determinants $\{\kappa_1\kappa_2\cdots\kappa_m\}_a=[q_1q_2\cdots q_m]_a$, we obtain from this and (9) the following proposition in determinants:*

$$a_r[q_1q_2\cdots q_r]=\Sigma[x_0, q_1+x_1, q_2+x_2, \cdots, q_r+x_r, \cdots, q_m], \tag{10}$$

where $x_0+x_1+x_2+\cdots+x_r=r$, $0\leqq x_0\leqq q_1+x_1, \leqq q_2+x_2, \cdots$, and where the same number must not be added to two or more equal indices (q's).

3. When the number of elements in p and q is the same, we may find the coefficient by a single reduction by subtracting unity from each element of p and q, for the partitions of the reduced coefficient. We have

$$\left|\left[\begin{matrix}p_1p_2\cdots p_n\\q_1q_2\cdots q_n\end{matrix}\right]\right|=\left|\left[\begin{matrix}p_1-1\ p_2-1\cdots p_n-1\\q_1-1\ q_2-1\cdots q_n-1\end{matrix}\right]\right|. \tag{11}$$

If n be the number of elements in each partition the coefficient of weight w is reduced to one of weight $w-n$. Thus $\left|\left[\begin{smallmatrix}2^2 3\\124\end{smallmatrix}\right]\right|=\left|\left[\begin{smallmatrix}1^2 2\\13\end{smallmatrix}\right]\right|=2$, by the table for weight 4. This depends upon the invariance of the table treated of in § 4, 8., and is there explained.

4. We have also the two following particular recurrence formulas:

$$\left|\left[\begin{matrix}p_1p_2p_3\\q_1q_2\end{matrix}\right]\right|=\begin{matrix}1\\0\end{matrix}+\left|\left[\begin{matrix}p_1-1\,p_2-1\,p_3-1\\q_1-1\,q_2-2\end{matrix}\right]\right|, \tag{12}$$

* Cf., MUIR, *Vanishing Aggregates of Secondary Minors of a Persymmetric Determinant*, Transactions of the Royal Society of Edinburgh, vol. 40 (1902), pp. 511–533.

where $q_2 \geqq q_1 + 1$, and where in the first term 0 or 1 is to be taken according as any element of p is or is not greater than q_2. Similarly

$$(13) \qquad \left|\begin{bmatrix} p_1 p_2 p_3 p_4 \\ q_1^2 \end{bmatrix}\right| = \begin{matrix} 1 \\ 0 \end{matrix} + \left|\begin{bmatrix} p_1 - 1\, p_2 - 1\, p_3 - 1\, p_4 - 1 \\ (q_1 - 2)^2 \end{bmatrix}\right|.$$

These formulas are derived from two relations given by W. W. JOHNSON,* taken in connection with the before-mentioned invariance. The relations, using the present notation, are

$$(14) \qquad \frac{|0\, q_1 + 1\, q_2 + 2|}{|012|} = t_{q_2, q_1} + \alpha_1 \alpha_2 \alpha_3 \frac{|0\, q_1\, q_2|}{|012|},$$

$$(15) \qquad \frac{|0\,1\, q_1 + 2\, q_1 + 3|}{|0123|} = t_{q_1, q_1} + \alpha_1 \alpha_2 \alpha_3 \alpha_4 \frac{|0\,1\, q_1\, q_1 + 1|}{|0123|}.$$

Examples:

$$\left|\begin{bmatrix} 2^2 3 \\ 3\ 4 \end{bmatrix}\right| = 1 + \left|\begin{bmatrix} 1^2 2 \\ 2^2 \end{bmatrix}\right| = 1 + 1 = 2,$$

$$\left|\begin{bmatrix} 1^2 5 \\ 3\ 4 \end{bmatrix}\right| = 0 + \left|\begin{bmatrix} 4 \\ 2^2 \end{bmatrix}\right| = 0 + 0 = 0,$$

$$\left|\begin{bmatrix} 1^2 2^2 \\ 3^2 \end{bmatrix}\right| = 1 + \left|\begin{bmatrix} 1^2 \\ 1^2 \end{bmatrix}\right| = 1 + 1 = 2,$$

$$\left|\begin{bmatrix} 1^3 3 \\ 3^2 \end{bmatrix}\right| = 1 + \left|\begin{bmatrix} 2 \\ 1^2 \end{bmatrix}\right| = 1 + 0 = 1.$$

5. From the product table, (I), we have

$$(16) \qquad (p) \equiv \sum_{\kappa} \left|\begin{matrix} \kappa \\ p \end{matrix}\right| \{\kappa\}_t;$$

from the quotient table,

$$(17) \qquad \{\kappa\}_t \equiv \sum_{q} \left|\begin{matrix} q \\ \kappa \end{matrix}\right| (q),$$

hence

$$(18) \qquad (p) \equiv \sum_{\kappa} \left|\begin{matrix} \kappa \\ p \end{matrix}\right| \cdot \left(\sum_{q} \left|\begin{matrix} q \\ \kappa \end{matrix}\right| (q)\right).$$

Again from the quotient table

$$(19) \qquad a_p \equiv \sum_{\kappa} \left|\begin{matrix} p \\ \kappa \end{matrix}\right| \{\kappa\}_a.$$

From the product table

$$(20) \qquad \{\kappa\}_a \equiv \sum_{q} \left|\begin{matrix} \kappa \\ q \end{matrix}\right| a_q,$$

* *On a Formula of Reduction for Alternants of the Third Order*, American Journal of Mathematics, vol. 7 (1885) pp. 347–352. See also the same author's paper *On the Calculation of the Co-Factors of Alternants of the Fourth Order*, l. c. pp. 380–388.

hence

$$a_p \equiv \sum_\kappa \left\| \begin{matrix} p \\ \kappa \end{matrix} \right\| \cdot \left(\sum_q \left| \begin{matrix} \kappa \\ q \end{matrix} \right| a_q \right). \tag{21}$$

From either of the identities (18) or (21) follows the identity

$$\sum_\kappa \left| \begin{matrix} \kappa \\ p \end{matrix} \right| \cdot \left\| \begin{matrix} q \\ \kappa \end{matrix} \right\| \equiv \begin{matrix} 0 \\ 1 \end{matrix}, \tag{22}$$

according as $\begin{matrix} p \neq q \\ p = q \end{matrix}$. From (22) we derive the recurrence formula,

$$\left\| \begin{bmatrix} p \\ q \end{bmatrix} \right\| = - \sum_\kappa \left| \begin{matrix} \kappa \\ q \end{matrix} \right| \cdot \left\| \begin{matrix} p \\ \kappa \end{matrix} \right\|, \tag{23}$$

where κ goes from $1\,2\,3 \cdots m$ to the complex next preceding

$$q_1\, q_2 + 1\, q_3 + 2 \cdots q_m + m - 1.$$

Thus

$$\left\| \begin{bmatrix} 1^4 2 \\ 1^3 3 \end{bmatrix} \right\| = -(-1-3) = 4.$$

By the help of the product table one can by means of this recurrence formula calculate any line of the quotient table beginning at the left of the line. If the quotient table were given the product table might similarly be found by the same relation.

§ 3. *General formulas for the* $\| \begin{smallmatrix} p \\ \kappa \end{smallmatrix} \|$.

As in the product table, so also in the quotient table it has been possible to generalize certain of the coefficients by columns. Since

$$\frac{|\kappa_1 \kappa_2 \cdots \kappa_m|}{|01 \cdots m-1|} = \{\kappa_1 \kappa_2 \cdots \kappa_m\}_t = \{\kappa\}_t$$

and since the determinants $\{\kappa\}_t$ are given in the product table, we may assume as known the function $\{\kappa\}_t$, which gives all the coefficients in the column headed by the complex κ or, what is the same thing, by the partition q. Let n_{-r} denote the number of different ways of subtracting r units from the complex of exponents $p_1 p_2 \cdots p_m$ of the symmetric function (p), and let $(n_{-r})_{r_1 r_2 \cdots r_\lambda}$ where $r_1 + r_2 + \cdots + r_\lambda = r$, denote the number of ways of subtracting r units at a time from p, r_1 from one index, r_2 from another and so on. Then

$$n_{-r} = \sum (n_{-r})_{r_1 r_2 \cdots r_\lambda}. \tag{24}$$

Also it is evident that

$$\left\| \begin{matrix} p \\ \kappa \end{matrix} \right\| = f(n_0, n_{-1}, n_{-2}, \cdots) = f(n), \tag{25}$$

and the problem of determining the $\left\|\begin{smallmatrix} p \\ \kappa \end{smallmatrix}\right\|$ is a purely combinatorial one. In particular with $p_1 p_2 \cdots p_m = 0^{x_0} 1^{x_1} 2^{x_2} \cdots m^{x_m}$,

$$(26) \qquad n_0 = \binom{x_1 + \cdots + x_m}{0} = 1, \qquad (n_{-2})_2 = \binom{x_2 + \cdots + x_m}{1},$$

$$(27) \qquad n_{-1} = \binom{x_1 + \cdots + x_m}{1}, \qquad (n_{-2})_{11} = \binom{x_1 + \cdots + x_m}{2},$$

$$(28) \qquad n_{-2} = (n_{-2})_2 + (n_{-2})_{11} = \binom{x_2 + \cdots + x_m}{1} + \binom{x_1 + \cdots + x_m}{2},$$

$$(29) \qquad (n_{-3})_3 = \binom{x_3 + \cdots + x_m}{1}, \quad (n_{-3})_{21} = 2\binom{x_2 + \cdots + x_m}{2} + \binom{x_2 + \cdots + x_m}{1}\binom{x_1}{1},$$

$$(n_{-3})_{111} = \binom{x_1 + \cdots + x_m}{3},$$

$$(30) \qquad n_{-3} = (n_{-3})_3 + (n_{-3})_{21} + (n_{-3})_{111} = \binom{x_3 + \cdots + x_m}{1} + 2\binom{x_2 + \cdots + x_m}{2} + \binom{x_2 + \cdots + x_m}{1}\binom{x_1}{1} + \binom{x_1 + \cdots + x_m}{3},$$

We thus find for the following partitions q, $\{\kappa\}_t = F(t)$, and $f(n)$, together with the coefficient which holds for the entire column headed by the partition q, as shown by the table on page 007.

Example: By (35)

$$\left\| \begin{bmatrix} 1^3 2^2 \\ 1^2 5 \end{bmatrix} \right\| = \binom{4}{2} = 6.$$

§4. *The construction and properties of the table.*

1. The partitions are written horizontally and vertically as explained for the product table, I, with complexes of alternants or determinants corresponding to the several partitions heading the columns. The quotient table is read vertically downwards and not horizontally as in the case of the product table. The argument is taken from the horizontal line of complexes at the top of the table in the column headed by the complex κ. The quotient $|\kappa_1 \kappa_2 \cdots \kappa_m| \,/\, |0\,1 \cdots m-1|$, is equal to the sum of all the products got by multiplying each coefficient of the column into the symmetric function signified by the partition at the left of the line in which the coefficient occurs.

2. From the nature of division* it is seen that the first term in the quotient

*See MUIR, *The Theory of Determinants*, § 130, p. 177.

Partition	$F(t)$	$f(n)$	Coefficient
$(31)(n)$	t_n	n_0	1
$(32)(n-11)$	$t_1 t_{n-1} - t_n$	$n_{-1} - n_0$	$x_1 + \cdots + x_m - 1$
$(33)(n-22)$	$t_2 t_4 - t_1 t_5$	$n_{-2} - n_{-1}$	$\binom{x_1 + \cdots + x_m}{2} - \binom{x_1}{1}$
$(34)(n-33)$	$t_3 t_{n-3} - t_2 t_{n-2}$	$n_{-3} - n_{-2}$	$\binom{x_2 + \cdots + x_m}{2} + \binom{x_1 + \cdots + x_m}{3} - \binom{x_2}{1} - \binom{x_1}{2}$
$(35)(n-21^2)$	$t_1^2 t_{n-2} + t_n - t_1 t_{n-1} - t_2 t_{n-2}$	$1 - n_{-1} - n_{-2} + (n_{-2})_2 + 2(n_{-2})_{11}$	$\binom{x_1 + \cdots + x_m - 1}{2}$
$(36)(n-321)$	$t_1 t_{n-1} - t_3 t_{n-3} - t_1^2 t_{n-2} + t_1 t_2 t_3$	$n_{-1} - n_{-3} - (n_{-2})_2 - 2(n_{-2})_{11} + (n_{-3})_3 + 2(n_{-3})_{21} + 3(n_{-3})_{111}$	$\binom{x_1}{1}\binom{x_2 + \cdots + x_m}{1} - \binom{x_1}{1} - 2\binom{x_1}{2} + 2\binom{x_1 + \cdots + x_m}{3}$
$(37)(n-431)$			$\binom{x_2}{1} - \binom{2x_2 + x_3 + \cdots + x_m}{1}\binom{x_1 + \cdots + x_m - 1}{1} + \binom{x_2 + \cdots + x_m}{2} + 2\binom{x_2 + \cdots + x_m}{1}\binom{x_1 + \cdots + x_m - 1}{2} + \binom{x_1 + \cdots + x_m}{2} + \frac{3}{4}\binom{x_1 + \cdots + x_m}{3}\binom{x_1 + \cdots + x_m - 1}{1}$
$(38)(n-44)$			$\binom{x_2 - x_3}{1} - \binom{x_1 + \cdots + x_m}{1}\binom{x_2}{1} - \binom{x_1 + \cdots + x_m}{3} + \binom{x_2 + \cdots + x_m}{2} + \binom{x_2 + \cdots + x_m}{1}\binom{x_1 + \cdots + x_m - 1}{2} + \binom{x_1 + \cdots + x_m}{4}$

is the symmetric function (q), where $q = \kappa_1, \kappa_2 - 1, \cdots, \kappa_m - m + 1$; whence it follows that

$$\left|\begin{bmatrix} p \\ q \end{bmatrix}\right| = 0, \tag{39}$$

when p precedes q, and

$$\left|\begin{bmatrix} p \\ p \end{bmatrix}\right| = 1. \tag{40}$$

From (39) and (40) it follows that the table is contained in a triangle which fills up the remainder of the square with the product table; also that the hypotenuse which belongs in common to both tables, consists of ones.

3. Of the coefficients none can be negative. This can be seen from (9) in which no minus sign occurs in the summation. It can also be seen from the standpoint of the coefficients as coefficients in the product of the elementary functions by $|01 \cdots m-1|$. In the formation of this product, units must be laid on the complex in such a way that no inversions of order can arise among the elements of the resulting complexes.

4. The last column consists of ones; in the next to the last column the coefficient is one less than the number of elements in the partition at the left in the same horizontal line with it. In the third last column the coefficient is equal to the number of combinations of the number of elements taken two at a time, minus the number of elements equal to unity. In the column headed by the partition $(n - 21^2)$ the coefficient is equal to the number of combinations of one less than the number of elements in the partition at the left, taken two at a time. These and other like generalizations follow from formulas (31) to (38).

5. The diagonal line next to the hypotenuse is skew symmetrical with the corresponding diagonal of the product table. This follows at once from formula (23). It can also be seen by noticing that the first term of the first remainder in the process of division comes from changing the sign of the alternant next to the hypotenuse. As a consequence of this property no coefficient of the product table in the diagonal next to the hypotenuse can be positive.

6. It may be recalled that it was shown in I, § 4 (30), that the coefficients are those of Dr. Taylor's product table, when conjugate columns have been interchanged. This also assumes a rearrangement of Dr. Taylor's table according to the writer's method of ordering, as explained in I.

7. The last line of the table is symmetrical with respect to its middle element or elements, as the first line of the product table is symmetrical or skew symmetrical in the same way according as w is odd or even.* In fact

* To prove this we note, by the method of § 3, 2. I, that all coefficients in the first line will be zero, except those whose column partition consists of r units and the element $m-r$. The value of the coefficient is then, by § 3, 2. I,

$$\begin{bmatrix} m \\ 1^r m-r \end{bmatrix} = (-1)^r.$$

$$\left|\begin{bmatrix} 1^m \\ p_m p_{m-1}\cdots p_2 p_1 \end{bmatrix}\right| = \left|\begin{bmatrix} 1^{m-1} \\ p_m p_{m-1}\cdots p_2 p_1 - 1 \end{bmatrix}\right| + \left|\begin{bmatrix} 1^{m-1} \\ p_m p_{m-1}\cdots p_2 - 1 p_1 \end{bmatrix}\right| + \cdots + \left|\begin{bmatrix} 1^{m-1} \\ p_m - 1 p_{m-1}\cdots p_1 \end{bmatrix}\right|, \tag{41}$$

$$\left|\begin{bmatrix} 1^m \\ 1^{p_1-p_2} 2^{p_2-p_3}\ldots m^{p_m} \end{bmatrix}\right| = \left|\begin{bmatrix} 1^{m-1} \\ 1^{p_1-1-p_2} 2^{p_2-p_3}\ldots m^{p_m} \end{bmatrix}\right| + \left|\begin{bmatrix} 1^{m-1} \\ 1^{p_1+1-p_2} 2^{p_2-1-p_3}\ldots m^{p_m} \end{bmatrix}\right| + \cdots + \left|\begin{bmatrix} 1^{m-1} \\ 1^{p_1-p_2} 2^{p_2-p_3}\ldots (m-1)^{p_{m-1}+1-p_m} m^{p_m-1} \end{bmatrix}\right|. \tag{42}$$

From (41) and (42), since the lower partitions of the left members and also of the right members term by term are conjugates, it follows, if the property is true for the table of weight $w-1$, it is true for the table of weight w. But it is seen to be true when $w=2$, and hence it is true for all values of w.*

8. Like the product table it possesses the invariant property. In fact since each is the unique inverse of the other table, the invariance of the quotient table follows from that of the product table. It also appears as follows. We have

$$\frac{|\kappa_1 \kappa_2 \cdots \kappa_m|}{|01\cdots m-1|} = \{\kappa\}_t = [q]_t. \tag{43}$$

If $i_1 i_2 \cdots i_{m+r}$ are so taken that

$$i_1,\ i_2-1,\ i_3-2,\ \cdots,\ i_{m+r}-m-r-1 = 0^r q_1 q_2 \cdots q_m,$$

then as an explicit function of t,

$$\frac{|i_1 i_2 \cdots i_{m+r}|}{|01\cdots m+r-1|} = \{\kappa\}_t = [q]_t. \tag{44}$$

Hence, in their development in terms of monomial symmetric functions, as far as these functions contain no more than m elements, $|i_1 i_2 \cdots i_{m+r}|/|01\cdots m+r-1|$ and $|\kappa_1 \kappa_2 \cdots \kappa_m|/|01\cdots m-1|$ must have identical coefficients. In the former the symmetric functions are functions of $m+r$ quantities $\alpha_1, \alpha_2, \cdots, \alpha_{m+r}$, in the latter they are functions of the m quantities $\alpha_1, \alpha_2, \cdots, \alpha_m$. The latter quotient can be obtained from the former by putting $\alpha_{m+1} = \alpha_{m+2} = \cdots = \alpha_{m+r} = 0$

* The value of the conjugate coefficient is

$$\left[\begin{matrix} m \\ 1^{m-r-1}(r+1) \end{matrix}\right] = (-1)^{m+r+1},$$

whence

$$\left[\begin{matrix} m & \cdot \\ 1^r & m-r \end{matrix}\right] = (-1)^{m+1}\left[\begin{matrix} m \\ 1^{m-r-1}(r+1) \end{matrix}\right],$$

which proves the proposition.

in it. It is also evident that (44) and its development are invariant if all the indices of both numerator and denominator be increased by the same positive integer λ.

9. If n_p denote the number of terms in the symmetric function (p), then $\sum n_p \left\| \begin{matrix} p \\ \kappa \end{matrix} \right\|$ is the whole number of terms in the quotient $|\kappa_1 \kappa_2 \cdots \kappa_m| / |01 \cdots m-1|$. But this number is equal to the difference product of the κ's divided by the difference product of $0, 1, 2, \cdots, m-1$ * hence we have the formula

$$(45) \qquad \sum_p \frac{n!}{x_0!\, x_1!\, x_2! \cdots x_m!} \left\| \begin{matrix} p \\ \kappa \end{matrix} \right\| = \frac{(\kappa_m - \kappa_1)(\kappa_m - \kappa_2) \cdots (\kappa_2 - \kappa_1)}{1!\, 2! \cdots (m-1)!},$$

as a farther relation and check for the coefficients of the quotient table.

§ 5. *The Quotient Table as a Table for Elementary Products (as a Product Table).*

A two-fold application of the table gives the elementary products in terms of monomial symmetric functions. Since $|\kappa_1 \kappa_2 \cdots \kappa_m| / |01 \cdots m-1| = \{\kappa\}_t$, the table gives the values of the determinants $\{\kappa\}_t$, in terms of monomial symmetric functions (formula (17)). Also since (I, (41)),

$$(46) \qquad \{\kappa\}_a = (-1)^w a_0^w \{\bar{\kappa}\}_t,$$

it gives the values of the determinants $\{\kappa\}_a$ in terms of monomial symmetric functions.

Thus

$$(47) \qquad \begin{aligned} [6]_a &= [1^6]_t = (1^6), \\ [15]_a &= [1^4 2]_t = 5(1^6) + (1^4 2), \\ [24]_a &= [1^2 2^2]_t = 9(1^6) + 3(1^4 2) + (1^2 2^2), \end{aligned}$$

with $a_0 = 1$.

Moreover, looked upon as a product table in Dr. Taylor's sense and read horizontally, it gives, by the application of the theorem of corresponding matrices, the elementary products directly in terms of the $\{\kappa\}_a$, (19), or, after multiplying the coefficients by $(-1)^w$ and using conjugate headings, in terms of the $\{\kappa\}_t$. In combination with the product table this gives the elementary products in terms of elementary products and thus leads to the identity (21), or it gives the elementary products developed in terms of the t's:

$$(48) \qquad a_p \equiv \sum_\kappa \left\| \begin{matrix} p \\ \kappa \end{matrix} \right\| \cdot \left(\sum_q \left\| \begin{matrix} \bar{\kappa} \\ q \end{matrix} \right\| t_q \right).$$

* O. H. MITCHELL, *Note on Determinants of Powers*, American Journal of Mathematics, vol. 4 (1881), p. 341.

By the use of conjugate alternants as headings, it gives directly the product of $|01\cdots m-1|$ and the elementary symmetric functions.

Examples:

$$(49)\qquad |012345|(1^4)(1^2)=|123456|+|023457|+|013467|.$$

$$(50)\qquad \begin{aligned}(1^4)(1^2)&=[24]_a+[15]_a+[6]_a\\&=[1^22^2]_t+[1^42]_t+[1^6]_t\\&=(1^22^2)+4(1^42)+15(1^6)\quad[\text{by (47)}].\end{aligned}$$

§ 6. *Tables.*

Quotient tables from weight one to weight seven inclusive are given below With each table is also given the product table. The latter consists of the diagonal of ones and the triangle of coefficients above this diagonal, while the quotient table consists of the same diagonal and triangle of coefficients below it. The quotient table is read as explained in § 4, 1, the product table as explained in I.

WEIGHT 1.

	1 (1)
(1)	**1**

WEIGHT 2.

	12 (1^2)	03 (2)
(2)	−1	**1**
(1^2)	**1**	1

WEIGHT 3.

	123 (1^3)	024 (21)	015 (3)
(3)	1	−1	**1**
(21)	−2	**1**	1
(1^3)	**1**	2	1

WEIGHT 4.

	1234 (1^4)	0235 (21^2)	0145 (2^2)	0136 (31)	0127 (4)
(4)	−1	1	0	−1	**1**
(31)	2	−1	−1	**1**	1
(2^2)	1	−1	**1**	1	1
(21^2)	−3	**1**	1	2	1
(1^4)	**1**	3	2	3	1

WEIGHT 5.

	12345 (1^5)	02346 (21^3)	01356 (2^21)	01347 (31^2)	01257 (32)	01248 (41)	01239 (5)
(5)	1	−1	0	1	0	−1	**1**
(41)	−2	1	1	−1	−1	**1**	1
(32)	−2	2	−1	−1	**1**	1	1
(31^2)	3	−1	−1	**1**	1	2	1
(2^21)	3	−2	**1**	1	2	2	1
(21^3)	−4	**1**	2	3	3	3	1
(1^5)	**1**	4	5	6	5	4	1

WEIGHT 6.

	123456 (1⁶)	023457 (21⁴)	013467 (2²1²)	012567 (2³)	013458 (31³)	012468 (321)	012459 (41²)	012378 (3²)	012369 (42)	01235 10 (51)	01234 11 (6)
(6)	−1	1	0	0	−1	0	1	0	0	−1	**1**
(51)	2	−1	−1	0	1	1	−1	0	−1	**1**	1
(42)	2	−2	1	−1	1	0	−1	−1	**1**	1	1
(3²)	1	−1	0	1	1	−1	0	**1**	1	1	1
(41²)	−3	1	1	1	−1	−1	**1**	0	1	2	1
(321)	−6	4	0	−2	−2	**1**	1	1	2	2	1
(31³)	4	−1	−1	0	**1**	2	3	1	3	3	1
(2³)	−1	1	−1	**1**	0	2	1	1	3	2	1
(2²1²)	6	−3	**1**	1	1	4	3	2	4	3	1
(21⁴)	−5	**1**	3	2	4	8	6	3	6	4	1
(1⁶)	**1**	5	9	5	10	16	10	5	9	5	1

WEIGHT 7.

	1234567 (1⁷)	0234568 (21⁵)	0134578 (2²1³)	0124678 (2³1)	0134569 (31⁴)	0124579 (321²)	0123679 (32²)	012456 10 (41³)	012389 (3²1)	012367 10 (421)	012356 11 (51²)	012348 10 (43)	012347 11 (52)	012346 12 (61)	012345 13 (7)
(7)	**1**	−1	0	0	1	0	0	−1	0	0	1	0	0	−1	**1**
(61)	−2	1	1	0	−1	−1	0	1	0	1	−1	0	−1	**1**	1
(52)	−2	2	−1	1	−1	0	−1	1	1	0	−1	−1	**1**	1	1
(43)	−2	2	0	−1	−2	1	1	1	−1	−1	0	**1**	1	1	1
(51²)	3	−1	−1	−1	1	1	1	−1	0	−1	**1**	0	1	2	1
(421)	6	−4	0	0	2	1	−1	−2	−1	**1**	1	1	2	2	1
(3²1)	3	−2	−1	2	2	−1	−1	0	**1**	1	1	2	2	2	1
(41³)	−4	1	1	1	−1	−1	0	**1**	0	2	3	1	3	3	1
(32²)	3	−3	2	−1	1	−1	**1**	0	1	2	1	2	3	2	1
(321²)	−12	6	1	−2	−3	**1**	1	1	2	4	3	3	4	3	1
(31⁴)	5	−1	−1	0	**1**	3	2	4	3	8	6	4	6	4	1
(2³1)	−4	3	−2	**1**	0	2	3	1	3	6	3	4	5	3	1
(2²1³)	10	−4	**1**	2	1	6	5	4	6	11	6	6	7	4	1
(21⁵)	−6	**1**	4	5	5	15	10	10	11	20	10	9	10	5	1
(1⁷)	**1**	6	14	14	15	35	21	20	21	35	15	14	14	6	1

SYRACUSE UNIVERSITY, *May*, 1904.

GENERAL THEORY OF CURVES ON RULED SURFACES*

BY

E. J. WILCZYNSKI†

§ 1. *Relation between the differential equations of the surface and of the curves situated upon it.*

Let a ruled surface be given by means of the system of differential equations

$$\begin{aligned} y'' + p_{11}y' + p_{12}z' + q_{11}y + q_{12}z = 0, \\ z'' + p_{21}y' + p_{22}z' + q_{21}y + q_{22}z = 0, \end{aligned} \tag{1}$$

so that the curves C_y and C_z will be two curves upon it, the lines joining corresponding points of these two curves being generators of the surface. We shall eliminate once z and once y, so as to obtain the linear differential equations of the fourth order which each of these functions must satisfy.

We have from (1), by differentiation,

$$\begin{aligned} y^{(3)} = r_{11}y' + r_{12}z' + s_{11}y + s_{12}z, \\ z^{(3)} = r_{21}y' + r_{22}z' + s_{21}y + s_{22}z, \end{aligned} \tag{2}$$

where

$$\begin{aligned} r_{11} &= p_{11}^2 + p_{12}p_{21} - p_{11}' - q_{11}, & s_{11} &= p_{11}q_{11} + p_{12}q_{21} - q_{11}', \\ r_{12} &= p_{12}(p_{11} + p_{22}) - p_{12}' - q_{12}, & s_{12} &= p_{11}q_{12} + p_{12}q_{22} - q_{12}', \\ r_{21} &= p_{21}(p_{11} + p_{22}) - p_{21}' - q_{21}, & s_{21} &= p_{21}q_{11} + p_{22}q_{21} - q_{21}', \\ r_{22} &= p_{22}^2 + p_{12}p_{21} - p_{22}' - q_{22}, & s_{22} &= p_{21}q_{12} + p_{22}q_{22} - q_{22}'. \end{aligned} \tag{3}$$

We find, by another differentiation,

$$\begin{aligned} y^{(4)} = l_{11}y' + l_{12}z' + m_{11}y + m_{12}z, \\ z^{(4)} = l_{21}y' + l_{22}z' + m_{21}y + m_{22}z, \end{aligned} \tag{4}$$

where

* Presented to the Society April 30, 1904. Received for publication March 12, 1904.

† Of the Carnegie Institution of Washington.

$$
\begin{aligned}
l_{11} &= -p_{11}r_{11} - p_{21}r_{12} + r'_{11} + s_{11}, & m_{11} &= -r_{11}q_{11} - r_{12}q_{21} + s'_{11},\\
l_{12} &= -p_{12}r_{11} - p_{22}r_{12} + r'_{12} + s_{12}, & m_{12} &= -r_{11}q_{12} - r_{12}q_{22} + s'_{12},\\
l_{21} &= -p_{11}r_{21} - p_{21}r_{22} + r'_{21} + s_{21}, & m_{21} &= -r_{21}q_{11} - r_{22}q_{21} + s'_{21},\\
l_{22} &= -p_{12}r_{21} - p_{22}r_{22} + r'_{22} + s_{22}, & m_{22} &= -r_{21}q_{12} - r_{22}q_{22} + s'_{22}.
\end{aligned} \tag{5}
$$

If we put further

$$
\Delta_1 = p_{12}s_{12} - q_{12}r_{12}, \qquad \Delta_2 = p_{21}s_{21} - q_{21}r_{21}, \tag{6}
$$

we can find, from the above equations,

$$
\begin{aligned}
\Delta_1 z &= p_{12}y^{(3)} + r_{12}y'' + (p_{11}r_{12} - p_{12}r_{11})y' + (q_{11}r_{12} - p_{12}s_{11})y,\\
-\Delta_1 z' &= q_{12}y^{(3)} + s_{12}y'' + (p_{11}s_{12} - q_{12}r_{11})y' + (q_{11}s_{12} - q_{12}s_{11})y,
\end{aligned} \tag{7}
$$

and similarly,

$$
\begin{aligned}
\Delta_2 y &= p_{21}z^{(3)} + r_{21}z'' + (p_{22}r_{21} - p_{21}r_{22})z' + (q_{22}r_{21} - p_{21}s_{22})z,\\
-\Delta_2 y' &= q_{21}z^{(3)} + s_{21}z'' + (p_{22}s_{21} - q_{21}r_{22})z' + (q_{22}s_{21} - q_{21}s_{22})z.
\end{aligned} \tag{8}
$$

Finally, we obtain the required differential equations for y and z, viz:

$$
\begin{aligned}
\Delta_1 y^{(4)} &= (p_{12}m_{12} - q_{12}l_{12})y^{(3)} + (r_{12}m_{12} - s_{12}l_{12})y''\\
&\quad + [(p_{11}r_{12} - p_{12}r_{11})m_{12} - (p_{11}s_{12} - q_{12}r_{11})l_{12} + \Delta_1 l_{11}]y'\\
&\quad + [(q_{11}r_{12} - p_{12}s_{11})m_{12} - (q_{11}s_{12} - q_{12}s_{11})l_{12} + \Delta_1 m_{11}]y,
\end{aligned} \tag{9}
$$

and

$$
\begin{aligned}
\Delta_2 z^{(4)} &= (p_{21}m_{21} - q_{21}l_{21})z^{(3)} + (r_{21}m_{21} - s_{21}l_{21})z''\\
&\quad + [(p_{22}r_{21} - p_{21}r_{22})m_{21} - (p_{22}s_{21} - q_{21}r_{22})l_{21} + \Delta_2 l_{22}]z'\\
&\quad + [(q_{22}r_{21} - p_{21}s_{22})m_{21} - (q_{22}s_{21} - q_{21}s_{22})l_{21} + \Delta_2 m_{22}]z.
\end{aligned} \tag{10}
$$

These equations are capable of a vast number of applications. Any question, in fact, in regard to the existence of curves of a specified character on a ruled surface must make use of them.

We notice that the conditions $\Delta_1 = 0$ or $\Delta_2 = 0$ will be necessary and sufficient to make C_y or C_z plane curves; the differential equations (of the third order) of these plane curves are found by putting $\Delta_1 = 0$ or $\Delta_2 = 0$ in (7) or (8) respectively. We will merely indicate a few other applications of these formulas. Let us write (9), more briefly,

$$
y^{(4)} + 4p_1y^{(3)} + 6p_2y'' + 4p_3y' + p_4y = 0. \tag{9'}
$$

It is easy to write down the conditions that the integral curve of (9′) shall belong to a linear complex, or that it shall be a twisted cubic. In one case its invariant of weight 3, and in the other both of its invariants, must vanish. But

these conditions, which we now find expressed in terms of the coefficients of (1), become conditions for a particular kind of ruled surface, which contains such curves. One can impose other conditions, for example, that these curves shall be flecnode curves or asymptotic curves on the surface, and then proceed to study the particular class of surface characterized.

It is not our intention to follow up any of these *special* problems, interesting as they are. We shall, however, apply our equations for the purpose of answering some questions of a fundamental nature in the *general* theory of ruled surfaces.

§ 2. *On ruled surfaces, one of the branches of whose flecnode curve is given.*

The flecnode curve is so important in the general theory of ruled surfaces, that it seems essential to investigate to what extent it may be arbitrarily assigned.

If one of the sheets of the flecnode surface, F', of S is given, there remain only two possibilities for S, namely, one or the other of the two sheets of the flecnode surface of F'. But let us suppose that we merely know that a certain curve C is one of the branches of the flecnode curve on S. Then there are two questions to answer. Can this curve be chosen arbitrarily? And how far does it determine the surface S?

Let the curve C be given by means of its differential equation

$$\frac{d^4\bar{y}}{d\bar{x}^4} + 4\bar{p}_1\frac{d^3\bar{y}}{d\bar{x}^3} + 6\bar{p}_2\frac{d^2\bar{y}}{d\bar{x}^2} + 4\bar{p}_3\frac{d\bar{y}}{d\bar{x}} + \bar{p}_4\bar{y} = 0, \tag{11}$$

where $\bar{p}_1, \cdots, \bar{p}_4$ are given functions of $\bar{x}$. In the system of differential equations (1) defining our surface S, we must regard the coefficients p_{ik} and q_{ik} as unknown functions. We may, however, assume without exception that $u_{12} = 0$, so that C_y is one of the branches of the flecnode curve on S, that $p_{21} = 0$, so that C_z is an asymptotic curve on S, and that $p_{11} = p_{22} = 0$. Under these assumptions we form the differential equation (9) of the curve C_y. Since C_y is to be identical with C it must be possible to convert equation (9) into (11) by a transformation of the form

$$y = \phi(x)\bar{y}, \qquad \bar{x} = f(x). \tag{12}$$

The functions ϕ and f are not independent however. For, while the equations $u_{12} = 0$ and $p_{21} = 0$ are not disturbed by any transformation of this form, the conditions $p_{11} = p_{22} = 0$ are. In fact a transformation of the form (12) converts (1) into another system of the same form whose corresponding coefficients $\bar{p}_{11}$ and $\bar{p}_{22}$ will be

$$\bar{p}_{11} = \frac{p_{11} + 2\dfrac{\phi'}{\phi} + \dfrac{f'''}{f'}}{f'}, \qquad \bar{p}_{22} = \frac{p_{22} + 2\dfrac{\phi'}{\phi} + \dfrac{f'''}{f'}}{f'}.$$

In order, therefore, that after this transformation $\bar{p}_{11}$ and $\bar{p}_{22}$ may again vanish, we must have

$$\phi = \frac{C}{\sqrt{f'}}, \tag{13}$$

where C is an arbitrary constant, which may be put equal to unity.

If then we apply the transformation (12) to (11), we shall get an equation

$$\frac{d^4y}{dx^4} + 4p_1\frac{d^3y}{dx^3} + 6p_2\frac{d^2y}{dx^2} + 4p_3\frac{dy}{dx} + p_4y = 0,$$

which we must identify with (9). Equating coefficients gives us a system of four equations with five unknown functions of x, viz.: f, p_{12}, q_{11}, q_{21}, q_{22}.

We find, therefore, the following theorem: *An arbitrary space curve being given, it can be considered as one branch of the flecnode curve of an infinity of ruled surfaces, into whose general expression there enters an arbitrary function.* One may, therefore, impose another condition and still obtain an infinity of ruled surfaces.

The most general curve C_z which is capable of being the second branch of the flecnode curve on a ruled surface for which C_y is the first branch, involves, therefore, in its expression one arbitrary function. It cannot, therefore, be an arbitrary curve, as that would involve three arbitrary functions.

Therefore, *two curves taken at random cannot be connected point to point in such a way as to constitute the complete flecnode curve upon the ruled surface thus generated.*

We can also prove our theorem by purely synthetic considerations. Let us take points $P_1, P_2, P_3, P_4, \cdots$ on an arbitrary curve, corresponding for example to equal increments Δx of the parameter. Through P_1, P_2, P_3 draw three arbitrary lines g_1, g_2, g_3. We can draw a line f_1 through P_1 intersecting g_2 and g_3, say in Q_2 and Q_3. Take an arbitrary point Q_4 on f_1, and join it to P_4 by a line g_4. Then f_1 intersects g_1, g_2, g_3, g_4. Through P_2 we draw a line f_2 intersecting g_3 and g_4 in points Q_3', Q_4' and of course g_2 in $Q_2' = P_2$. Take an arbitrary point Q_5' on f_2 and join it to P_5 by a line g_5. Continue this process. Clearly, we shall get two assemblages of lines $g_1, g_2, \cdots$ and $f_1, f_2, \cdots$, which when $P_1, P_2, \cdots$ are taken closer and closer together, approach as a limit two ruled surfaces having the given curve as flecnode curve, and which are flecnode surfaces of each other. The first three lines g_1, g_2, g_3 are arbitrary, and thus give rise to six constants of integration. Further, the double ratios (P_1, Q_2, Q_3, Q_4), (Q_2', Q_3', Q_4', Q_5'), etc., may be chosen arbitrarily, which brings into evidence the arbitrary function involved in the construction of these surfaces.

The construction which has just been described becomes indeterminate if the given curve C is a straight line. For then Q_4 coincides with P_4, etc. In fact,

the most general ruled surface with a given straight line directrix depends on two arbitrary functions.

If the given curve C is to be at the same time the second branch of the flecnode curve, i. e., if both of the branches of the flecnode curve of S coincide with C, g_4 must be tangent to the hyperboloid determined by g_1, g_2, g_3; g_5 must be tangent to the hyperboloid determined by g_2, g_3, g_4; etc. This condition, therefore, clearly fixes the double ratios $(Q_1 Q_2 Q_3 Q_4)$, etc., i. e., the arbitrary function. Therefore this problem has in general ∞^6 solutions.

Let us assume that C_y is not a straight line. Let us call the developable surface formed by the tangents of C_y its *primary* developable. There exists another important developable surface containing C_y, which we shall speak of as its *secondary* developable, as indicated in the following theorem.

1. *If at every point of the flecnode curve of S there be drawn the generator of the surface, the flecnode tangent, the tangent of the flecnode curve, and finally the line which is the harmonic conjugate of the latter with respect to the other two, the locus of these last lines is a developable surface, the secondary developable of the flecnode curve.*

2. *We can find a single infinity of ruled surfaces, each having one branch of its flecnode curve in common with that of S. This family of ∞^1 surfaces can be described as an involution, of which any surface of the family and its flecnode surface form a pair. The primary and secondary developables of the branch of the flecnode surface considered, are the double surfaces of this involution. In fact, the generators of these surfaces, at every point of their common flecnode curve, form an involution in the usual sense.*

We proceed to prove these theorems. Since C_y is a branch of the flecnode curve, we may assume $u_{12} = p_{11} = p_{22} = 0$. System (1) assumes the form

$$(14) \qquad y'' + p_{12}z' + q_{11}y + \tfrac{1}{2}p'_{12}z = 0, \qquad z'' + p_{21}y' + q_{21}y + q_{22}z = 0.$$

The flecnode tangent at P_y is the line joining P_y to P_ρ, where

$$\rho = 2y' + p_{12}z,$$

while the tangent of the flecnode curve joins P_y to $P_{y'}$. In the plane pencil formed by these lines, the harmonic conjugate of $P_y P_{y'}$ with respect to $P_y P_z$ and $P_y P_\rho$ will be the line $P_y P_\tau$, where

$$\tau = y' + p_{12}z.$$

But from the first equation of (14) we find

$$(15) \qquad \tau' + q_{11}y - \tfrac{1}{2}\frac{p'_{12}}{p_{12}}(\tau - y') = 0,$$

i. e., $P_y P_\tau$ generates a *developable* surface as asserted in the first theorem.

Put

$$\begin{aligned} e &= \tau + ky' = (1+k)y' + p_{12}z, \\ f &= \tau - ky' = (1-k)y' + p_{12}z, \end{aligned} \tag{16}$$

where k is a constant. Clearly the lines P_yP_e and P_yP_f form a pair of the involution whose double lines are $P_yP_{y'}$ and P_yP_τ.

One finds that y and e satisfy the following system of differential equations:

$$\begin{aligned} y'' + P_{11}y' + P_{12}e' + Q_{11}y + Q_{12}e &= 0, \\ e'' + P_{21}y' + P_{22}e' + Q_{21}y + Q_{22}e &= 0, \end{aligned} \tag{17}$$

where

$$P_{11} = -\frac{1+k}{2k}\frac{p'_{12}}{p_{12}}, \quad P_{12} = -\frac{1}{k}, \quad Q_{11} = -\frac{q_{11}}{k}, \quad Q_{12} = \frac{1}{2k}\frac{p'_{12}}{p_{12}},$$

$$P_{21} = (1+k)q_{11} + k(1+k)q_{22} - kp_{12}p_{21} + \frac{(1-3k)(1-k^2)}{4k}\left(\frac{p'_{12}}{p_{12}}\right)^2 + \frac{1-k^2}{2}\frac{p''_{12}}{p_{12}},$$

$$P_{22} = \frac{1-3k}{2k}\frac{p'_{12}}{p_{12}}, \tag{18}$$

$$Q_{21} = (1+k)q'_{11} - kp_{12}q_{21} + \frac{(1-3k)(1+k)}{2k}\frac{p'_{12}}{p_{12}}q_{11},$$

$$Q_{22} = -\left[kq_{22} + \frac{(1-3k)(1-k)}{4k}\left(\frac{p'_{12}}{p_{12}}\right)^2 + \frac{1-k}{2}\frac{p''_{12}}{p_{12}}\right].$$

We find

$$U_{12} = 2P'_{12} - 4Q_{12} + P_{12}(P_{11} + P_{22}) = 0,$$

i. e., the curve C_y is flecnode curve on the ruled surface S_k generated by P_yP_e. The flecnode surface of S_k is obtained by joining P_y to the point

$$2y' + P_{11}y + P_{12}e = -\frac{1}{k}f - \frac{1+k}{2k}\frac{p'_{12}}{p_{12}}y,$$

a point on the line P_yP_f. We see therefore that the ruled surfaces S_k and and S_{-k} are flecnode surfaces of each other. We have now proved our second theorem, and we may speak of an involution of ruled surfaces having one branch of their flecnode curve in common. The double surfaces of the involution are developables, while the members of each pair of the involution are flecnode surfaces of each other.

We have seen that P_yP_τ generates a developable. If

$$g = \alpha y + \beta\tau$$

represents its edge of regression, it must be possible to represent g' in the form

$$g' = \gamma y + \delta\tau,$$

since the line P_yP_τ must then be tangent to the curve C_g.

We find, by differentiation, making use of (15),

$$g' = \alpha y' + \beta\left(\tfrac{1}{2}\frac{p'_{12}}{p_{12}}\tau - q_{11}y - \tfrac{1}{2}\frac{p'_{12}}{p_{12}}y'\right) + \alpha' y + \beta'\tau,$$

so that g' will be of the required form if, and only if,

$$\alpha : \beta = p'_{12} : 2p_{12}.$$

Therefore

$$g = p'_{12}y + 2p_{12}\tau.$$

If we express τ in terms of y, z and ρ, we shall find

$$g = p_{12}\rho + p'_{12}y + p^2_{12}z \tag{19a}$$

as the expression for the edge of regression of the secondary developable of the branch C_y of the flecnode curve. Similarly, if $\theta_4 \neq 0$,

$$h = p_{21}\sigma + p'_{21}z + p^2_{21}y \tag{19b}$$

will represent the cuspidal edge of the secondary developable of the branch C_z of the flecnode curve, assuming, of course, $u_{21} = 0$.

One easily finds

$$-\tfrac{3}{2}p'_{12}g + p_{12}g' = \lambda y, \qquad -\tfrac{3}{2}p'_{21}h + p_{21}h' = \mu z, \tag{20}$$

where

$$\begin{aligned}\lambda &= p_{12}p''_{12} + \tfrac{1}{2}p^2_{12}u_{11} - p^3_{12}p_{21} - \tfrac{3}{2}(p'_{12})^2,\\ \mu &= p_{21}p''_{21} + \tfrac{1}{2}p^2_{21}u_{22} - p^3_{21}p_{12} - \tfrac{3}{2}(p'_{21})^2.\end{aligned} \tag{21}$$

The system of differential equations of which g and h are the solutions has the coefficients

$$\begin{aligned}P_{11} &= -\frac{1}{\lambda}[\lambda' + \tfrac{3}{4}p^2_{12}p'_{12}p_{21}], \qquad P_{12} = \frac{p_{21}\lambda}{\mu}, \qquad Q_{12} = -\frac{3p'_{21}\lambda}{2\mu},\\ Q_{11} &= -\frac{1}{\lambda p_{12}}[\lambda(2p''_{12} + \tfrac{1}{4}p_{12}u_{11} - \tfrac{1}{2}p^2_{12}p_{21}) - \tfrac{3}{2}p'_{12}(\lambda' + \tfrac{3}{4}p^2_{12}p'_{12}p_{21})],\end{aligned} \tag{22}$$

while P_{21}, P_{22}, Q_{22}, Q_{21} are obtained from these same equations by permuting the indices 1 and 2, and consequently also the letters λ and μ.

We see that we thus obtain, corresponding uniquely to any ruled surface whose flecnode curve intersects every generator in two distinct points, another ruled surface which is generated by the lines joining corresponding points of the edges of regression of the secondary developables of the two branches of the flecnode curve.

Equations (20) show that one of the secondary developables of C_y and C_z degenerates into a cone if λ or μ vanishes. In that case our new ruled surface also becomes a cone. If both of the secondary developables are cones, this ruled

surface degenerates into the straight line joining their vertices. If $\lambda = \Delta_1 = 0$, the secondary developable of C_y is a plane pencil.

Equations (22) show that this new ruled surface cannot be developable except if λ or μ is zero, i. e., unless it is a cone. For the possibility $p_{12} = 0$ or $p_{21} = 0$ is to be excluded, since we should then have a ruled surface S with a straight line directrix.

§ 3. *On ruled surfaces one of the branches of whose complex curve is given.*

There exists an infinity of ruled surfaces each of which contains an arbitrarily given curve as one branch of its complex curve. Into the general analytical expression of these surfaces there enters an arbitrary function. The analytical proof of this statement is precisely similar to that of the corresponding theorem of § 2. We shall give at once a geometrical construction for these surfaces.

Let us consider five straight lines $g_1, \cdots, g_5$. Let f_1', f_1'' be the two transversals of $g_1, \cdots, g_4$, and f_2', f_2'' those of $g_2, \cdots, g_5$. Clearly $g_1, \cdots, g_5$ determine a linear complex, with respect to which f_1', f_1'' and f_2', f_2'' are two pairs of reciprocal polars. Take a point P on g_1. The plane, which corresponds to it in the linear complex, passes through g_1 and the line h, which passes through P and intersects both f_2' and f_2''. If $g_2, \cdots, g_5$ are made to approach each other, we shall have in the limit five consecutive generators of a ruled surface and its osculating linear complex. The plane tangent to this ruled surface at P is the limit of the plane containing g_1 and the line through P which intersect g_2 and g_3, i. e., the asymptotic tangent of the surface at P. If P is a point on the complex curve, h_1 must be in the plane tangent to the ruled surface at P.

Now let an arbitrary curve be given, and let us choose points upon it, $P_1, P_2, P_3, \cdots$, according to any law. Through $P_1, \cdots, P_4$ draw four arbitrary lines $g_1, \cdots, g_4$. Through P_1 draw h_1, any line which intersects g_2. Let Q be this point of intersection. The line g_5, through P_5, is to be constructed in such a way that the two transversals of $g_2, \cdots, g_5$ shall both meet h_1. Now these transversals must be generators of the second set on the hyperboloid determined by g_2, g_3, g_4. They must, therefore, be those two generators of the second set, f_2' and f_2'', which pass through the two points in which h_1 intersects the hyperboloid. One of these points is Q. There exists just one line through P_5 intersecting both f_2' and f_2''. It is the line g_5. In the same way, starting with $g_2, \cdots, g_5$, we can construct g_6, etc. Finally we pass to the limit. There enters an arbitrary function, fixing the position of the successive lines $h_1, h_2, \cdots$ in the planes in which they must lie.

That a corresponding theorem is true for asymptotic curves, is obvious.

NICE, *February* 25th, 1904.

THEORY ON PLANE CURVES IN NON-METRICAL ANALYSIS SITUS*

BY

OSWALD VEBLEN

§ 1. *Introduction.*

JORDAN'S † explicit formulation of the fundamental theorem that a simple closed curve lying wholly in a plane decomposes the plane into an inside and an outside region is justly regarded as a most important step in the direction of a perfectly rigorous mathematics. This may be confidently asserted whether we believe that perfect rigor is attainable or not. His proof, however, is unsatisfactory to many mathematicians. It assumes the theorem without proof in the important special case of a simple polygon ‡ and of the argument from that point on, one must admit at least that all details are not given.

The work of SCHOENFLIES,§ especially in formulating a converse theorem has thrown much light on its relation to the theory of point sets and Analysis Situs in general, and elegant proofs under restrictive hypotheses have been given by AMES ‖ and BLISS.** All these discussions make more or less use of the ideas of analysis, thus implying either an axiom to the effect that a plane is a doubly extended number-manifold or a set of congruence axioms. Either of these hypotheses imposes a restriction upon the formal generality of Analysis Situs as a science independent of the magnitude of the figures treated.

* Presented to the Society at the St. Louis meeting, September 17, 1904, under the title, *The fundamental theorem of Analysis Situs*. Received for publication August 22, 1904.

† C. JORDAN, *Cours d'Analyse*, Paris, 1893, 2d ed., p. 92.

‡ This case was under discussion at the University of Chicago in 1901–02 in connection with Professor MOORE's seminar on Foundations of Geometry. Mr. N. J. LENNES gave a proof in his master's thesis (1903), *Theorems on the simple polygon and polyhedron*. Another proof appears as theorem 28 in the writer's dissertation (for reference, see footnote below). The present paper owes much to the discussions of the subject that have taken place under the leadership of Professor MOORE.

§ A. SCHOENFLIES, *Ueber einen grundlegenden Satz der Analysis Situs*, Nachrichten der Göttinger Gesellschaft der Wissenschaften, 1902, p. 185; *Beiträge zur Theorie der Punktmengen*, Mathematische Annalen, Vol. 58 (1903), p. 195.

‖ L. D. AMES, *On the theorem of Analysis Situs relating to the division of the plane or of space by a closed curve or surface*, Bulletin of the American Mathematical Society (2), vol. 10 (1904), p. 301.

** G. A. BLISS, *The exterior and interior of a plane curve*, Bulletin of the American Mathematical Society (2), vol. 10 (1904), p. 398.

In the following pages an attempt is made to discuss the theorem of JORDAN and a number of related questions under considerably more general hypotheses than are employed in any of the works referred to above. This undertaking practically results in a statement in logical terms of a body of information that formerly was used without explicit formulation and recently has been cramped by unnecessary restrictions. In other words we are inquiring how wide may be the application of our intuitive notion of a plane curve.*

The arguments and definitions are based upon axioms I–VIII, XI of the system adopted in the writer's dissertation † to which refer all the citations not otherwise indicated. These axioms are sufficient to determine the intersectional properties of straight lines, the ordinal relations ‡ of points on a straight line, and continuity. We accordingly assume nothing about analytic geometry, the parallel axiom, congruence relations, nor the existence of points outside a plane. For example, the theory is as valid in the non-desarguesian geometries of HILBERT and MOULTON § as in the geometries of EUCLID and LOBATCHEWSKY, and is of course as applicable in pure analysis as in geometry. ‖

The reader who prefers the JORDAN definition of a simple curve (which according to § 4 is equivalent to ours for purposes of analysis) and does not care about the question of non-metrical hypotheses, may conveniently begin with § 5. A relatively simple proof of the theorem of JORDAN about the decomposition of the plane which applies to any simple closed curve having a straight line inter-

*The general problem of the "mathematics of precision" may be stated in similar terms.

†O. VEBLEN, *A System of Axioms for Geometry*, Transactions of the American Mathematical Society, vol. 5 (1904), pp. 343–384.

‡The line is open, i. e., between every two points there is a third, and the order ABC excludes BAC and ACB. Single elliptic geometry and projective geometry are therefore excluded unless a properly chosen cut is introduced.

§F. R. MOULTON, *A Simple non-desarguesian Geometry*, these Transactions, vol. 3 (1902), p. 192.

‖ As to the applicability of our results in analysis, it seems desirable to add a remark which, though obvious from the point of view of "foundations of mathematics," may be of service to some readers who are not directly interested in this point of view. Numerical analysis is ordinarily thought of as founded on the concept of the positive integers. In terms of these a proof of existence can be given of a set of elements, or quantities, satisfying the postulates of the system of rational numbers, positive and negative. In terms of the rational numbers, in turn, can be given a proof of the existence of elements satisfying the postulates of the continuous real number system. Finally, the processes of analysis have to do with pairs of real numbers (x, y). The set of all such number-pairs is a set of objects about which (with proper definition of the term "order") our axioms I–VIII, XI are true theorems. From the axioms of analysis, the line of deduction of our theorems is therefore clear and simple. Not only that, but we may add that any theorem or any definition rigorously based on the assumptions of geometry is *ipso facto* a theorem or definition of analysis. Such considerations as these justify the assertion that while much may be lost in elegance and simplicity, nothing is gained in rigor by the banishment of geometrical language and geometrical styles of exact reasoning from pure analysis. (Of course, under sufficiently strong geometrical axioms, these remarks may be reversed and applied to the rôle of analysis in geometry.)

val is to be obtained by considering theorem 8 applied to a triangular region, theorem 9 applied to a simple polygon, corollary 2 of theorem 9, lemma B, theorem 10 and lemma C. This "reduced proof" could in turn be slightly modified so as to apply to any curve having at least one non-cuspidal tangent.

§ 2. *Non-metrical definition of limit point.*

For the definition of the terms, triangle, polygon, broken line, triangular region, separate, decompose, the reader is referred to § 4, chapter II. Of the theorems there proved we assume for the present purpose only that a triangle decomposes a plane in which it lies into two regions, an interior and an exterior.

DEFINITION 1. A *triangular region* is the interior of a triangle. A *geometrical limit point* of a set of points, $[X]$,* in a plane is a point P such that every triangular region including P includes a point X, distinct from P. A *triangular region* including a point is called a *neighborhood* of the point.

The continuity axiom was assumed for only one segment of a straight line and proved by projection for all lines. In like manner by projection it can be proved that for every point, P, of any line there exists a numerably infinite set of segments $[\sigma_\nu]$ $(\nu = 1, 2, \cdots)$ such that σ_ν contains $\sigma_{\nu+1}$ and such that P is the only point that lies on every σ_ν. It is an easy consequence of this that for every point in a plane there exists a set of triangular regions $[t_\nu]$ with a similar property. We also prove without difficulty the theorem that a limit point of a set of limit points of a set of points, $[X]$, is itself a limit point of $[X]$.

DEFINITION 2. A *region* is a set of points, any two of which are points of at least one broken line composed entirely of points of the set. An *interior point* of a region, R, is one that can be surrounded by a triangle containing only points of R. Consequently, an interior point of R is a geometrical limit point of no set of points that does not contain points of R. A *frontier point* of a region R is a point or geometrical limit point of R not an interior point, i. e., it is a limit point both of R points and of not R points. An *exterior point* of R or a point exterior to R is any point neither an interior nor a frontier point of R. The *frontier* or *boundary* of a region is a set of all frontier points. An *open region* contains no frontier points. A *closed region* contains all its frontier points.

One of the most familiar examples of an open region is obtained by letting $[C]$ stand for a closed set of points and $[P]$ for the set of all points that can be joined with a point P_0 not of $[C]$ by broken lines not meeting $[C]$; $[P]$ is an open region.—It is to be noted that the points exterior to a region $[P]$, if such exist, need not constitute only a single region.

* The notation $[X]$ denotes a set of elements any one of which is denoted by X alone or with suffixes. If we wish to indicate that the set is *ordered* we use $\{X\}$ instead of $[X]$.

§ 3. *Definition of simple curve.*

Simple curves, closed and unclosed, are composed of sets of points subject to certain conditions which we arrange in the following groups:

A. LINEAR ORDER. Among the points of a set of points $\{P\}$ there exists a relation, $\odot$, which we may read *precedes*, such that:

1. $\{P\}$ *contains at least two points.*

2. *If* P_1 *and* P_2 *are any two distinct points of* $\{P\}$, *then either* $P_1 \odot P_2$ *or* $P_2 \odot P_1$.

3.* *If* $P_1 \odot P_2$, *then not* $P_2 \odot P_1$.

4. *If* $P_1 \odot P_2$ *and* $P_2 \odot P_3$, *then* $P_1 \odot P_3$.

B. ORDINAL CONTINUITY.

1. *If* P_1 *and* P_3 *are any two points of* $\{P\}$, *such that* $P_1 \odot P_3$, *then there is a point* P_2 *of* $\{P\}$ *such that* $P_1 \odot P_2$ *and* $P_2 \odot P_3$.

2. *If every point of* $\{P\}$ *belongs to* $[P_1]$ *or* $[P_2]$, *two infinite subsets of* $\{P\}$ *such that for every* P_1 *and* P_2, $P_1 \odot P_2$, *then there is a point* P' *such that for every* P_1 *and* P_2 *distinct from* P', $P_1 \odot P'$ *and* $P' \odot P_2$.

C. GEOMETRICAL CONTINUITY.

1. *Let* P_0 *be any point of* $\{P\}$ *for which there is an infinity of points* P' *such that* $P' \odot P_0$. *Denote the set of all such points by* $[P']$; *then for every triangular region,* t, *including* P_0, *there is a point of* $[P']$, P'_t *such that* t *includes all points of* $[P']$ *for which* $P'_t \odot P'$.

2. *Let* P_0 *be any point of* $\{P\}$ *for which there is an infinity of points* P'' *such that* $P_0 \odot P''$. *Denote the set of all such points by* $[P'']$; *then for every triangular region,* t, *including* P_0 *there is a point of* $[P'']$, P''_t *such that* t *includes all points of* $[P'']$ *for which* $P'' \odot P''_t$.

DEFINITION 3. By the term *arc* or *arc of curve* is meant a set of points $\{P\}$ satisfying conditions *A*, *B*, *C* and including two points P_1, P_2 such that every point P, distinct from P_1 and P_2, satisfies the further conditions that $P_1 \odot P$ and $P \odot P_2$. The arc is said to *join* P_1 and P_2 which are called its *end-points.*

DEFINITION 4. A *simple closed curve*, j, is a set of points, $\{J\}$, consisting of two arcs joining two points J_1 and J_2 but having in common no points other than J_1, J_2.

THEOREM 1. *Any two points of* j *may be taken as the points,* J_1, J_2 *in the above definition.*

The proof of this theorem is here omitted as it involves no difficulty. The existence of sets of points satisfying the conditions of our definitionis proved by the examples of an interval of a straight line, which is an arc, and the boundary of a simple polygon, which is a simple closed curve. We shall use the letter j,

*From this it follows that if $P_1 \odot P_2$, then $P_1 \neq P_2$.

to denote a simple closed curve, in honor of CAMILLE JORDAN. The term *arc* of course does not cover the most general case of an unclosed curve. On the other hand the conditions A, B, C are too general to define an unclosed curve since they are satisfied, for example, by the boundary of a triangle exclusive of one vertex. We therefore set down the following condition which is evidently satisfied by an arc.

DEFINITION 5. A *simple unclosed curve* is a set of points $\{C\} = c$ that satisfies conditions A, B, C and also the following:

D. If C is any point of the curve, no point except C is a limit point (in the geometrical sense of definition 1) *both of the set of all points C' such that $C' \circledcirc C$ and of the set of all points C'' such that $C \circledcirc C''$.*

Any simple closed or simple unclosed curve is called a *simple curve*. For a set of points satisfying conditions A, B and C, it is evident that there hold all the propositions usually proved in the theory of linear point-sets with the exception of those that involve the length of intervals. We may mention particularly the propositions of section 5, chapter II, including the HEINE-BOREL theorem and the definition of ordinal limit point, the properties of point-free intervals in connection with closed sets, and the proposition that a line cannot be separated into two subsets each of which includes all its limit points. We do not stop here to prove these propositions though we make use of the last one in the following theorem.

DEFINITION 6. A relation satisfying conditions A, B, C is called a *sense*. A sense in which $P_1 \circledcirc P_2$ is said to be *from* P_1 *to* P_2.

THEOREM 2. *From one point to another upon a simple unclosed curve there is one and but one sense, while upon a simple closed curve there are two and but two senses.*

Proof. We have to show that if ρ is any relation satisfying the conditions A, B, C and D imposed on $\circledcirc$, then if $P_1 \rho P_2$ implies for one pair $P_1 P_2$ of $\{P\}$ that $P_1 \circledcirc P_2$, $P_1 \rho P_2$ implies that $P_1 \circledcirc P_2$ for every pair $P_1 \rho P_2$ of $\{P\}$.

If P_1 is any point of $\{P\}$, let $[P']$ be the set of all points such that simultaneously $P_1 \rho P'$ and $P_1 \circledcirc P'$. Every limit point $\bar{P}$ $(\bar{P} \neq P_1)$ of $[P']$ with respect to the sense ρ must by conditions A, B and C be such that $P_1 \rho P'$. Moreover P, by condition C, is a geometrical limit point of $[P']$. But in view of condition D, P being a point of $\{P\}$ and a geometrical limit point of points P' such that $P_1 \circledcirc P'$ must be such that $P_1 \circledcirc P$; otherwise P $(P \neq P_1)$ would be a geometrical limit point both of points $\bar{P}$ such that $\bar{P} \circledcirc P_1$ and of points P' such that $P_1 \circledcirc P'$.

Therefore the set $[P']$, if existent, contains all its limit points with respect to the sense ρ, except the point P_1. Similarly the set of all points P'', such that simultaneously $P_1 \rho P''$ and $P'' \circledcirc P_1$ must, if existent, contain all its limit points with respect to the sense ρ. Therefore, since the set of points $\{P_2\}$

such that $P_1 < P_2$ cannot consist of two subsets, each closed with the exception of P_1, every point P_2 must either be such that $P_1 \odot P_2$ or every point P_2 must be such that $P_2 \odot P_1$. From this result the conclusion of our theorem follows at once.

DEFINITION 7. If with respect to any sense on a curve, $P_1 \odot P_2$ and $P_2 \odot P_3$, P_2 is *between* P_1 and P_3 in that sense. The set of all points between P_1 and P_3 in the given sense is called a *segment* $P_1P_2P_3$ whose *end-points* are P_1, P_3. The segment and its end-points together constitute an *arc* or *interval* of the curve. On a simple unclosed curve, if $P_1 \odot P_2 \odot P_3$, P_2 is said to *separate* P_1 and P_3. On any simple curve if $P_1 \odot P_2 \odot P_3 \odot P_4$, P_1 and P_3 are said to separate and be separated by P_2 and P_4. If a set $[P_\nu]$ $(\nu = 1, 2, 3, \cdots)$ is such that $P_\nu \odot P_{\nu+1}$, the points P_ν are said to be in *the order along the curve*, $P_1P_2P_3 \cdots P_\nu P_{\nu+1} \cdots$. A point P_0 is the *first* of a set $[P]$ if $P_0 \odot P$ for every $P \neq P_0$; P_1 is the *last* of the set $[P]$ if $P \odot P_1$ for every $P \neq P_1$.

Either of the relations of "betweenness" or "separation" which are here defined in terms of "precedence" could have been used as fundamental* and a definition of a simple curve equivalent to the above would have resulted. The deduction of the properties of these relations will be omitted.

§ 4. *Remarks on the definition of a simple closed curve.*

While the definitions of the preceding section are stated so as to apply only to plane curves, it is obvious that if one replaces triangles by tetrahedrons or the corresponding figures in space of more dimensions, the conditions A, B, C, etc., give a definition of a simple curve in space of any number of dimensions.

It may be of interest to note that when one passes from the realm of plane geometry, the distinction between metric and non-metric theory loses much of its importance. For if we add to our assumptions (axioms I–VIII, XI) the assumption (axiom IX) that there exists a point outside a plane, then it is possible to define the ideal elements of projective geometry (cf. chapter III) and by choosing among these ideal elements an "absolute" plane† and polar system to establish a projective theory of congruence. We are thus enabled to operate in the most general case by ordinary analytic geometry as if dealing with the whole or a limited region of euclidean space.

As to the relation of the above definition to the current definition‡ in terms of a numerical parameter, it has not yet been determined whether, in the presence of axioms I–VIII, XI alone, the two definitions are or are not equivalent.

*Cf. B. RUSSELL, *The Principles of Mathematics*, Cambridge, 1903, chapters 24, 25. On the definition by postulate of "separation," see G. VAILATI, *Sulle relazioni di posizione tra punti d'una linea chiusa*, Rivista di Matematica, vol. 5 (1895), p. 75; and also ibid., p. 183.

†That there always is an ideal plane depends in particular on axioms III and XI which determine that straight lines shall be open.

‡See JORDAN, loc. cit. p. 90.

If however we introduce axiom IX as indicated above or bring in a set of congruence axioms like HILBERT's group IV, then the two definitions can be shown to be equivalent by reference to a theorem of CANTOR.*

Let a be any arc of a simple closed curve j. The points of a, excluding the end points, evidently constitute what CANTOR calls a *perfect* set, i. e., with respect to the sense $\ominus$. Let $\{t_n\}$ denote a set of equilateral triangles concentric and similarly placed such that the lengths of the side of t_n is $1/n$. For every point J of a there is such a set of triangles $\{t_n\}_J$, having J as a common center. Each triangle t_n determines an arc i_n of j which lies wholly within t_n (cf. condition C) and includes the central point J of t_n. Among the arcs i_n, there is by the HEINE-BOREL theorem applied to a, a finite subset such that every point of a is interior to one of the arcs i_n. The end points of these arcs that lie on a, excluding the end points of a, we denote by

$$A_n^1, A_n^2, \cdots, A_n^{m_n}.$$

The set of points $\{A_n^k\}$ is evidently numerable, is ordered according to one of the senses of a, and moreover is *everywhere dense on* a. For if it were not everywhere dense on a there would be some interval i of a which for *every* n lies wholly within *some* i_n and therefore within some t_n; whereas two of its points are a certain distance apart greater than $1/n$ for n sufficiently great.

Now by the theorem of CANTOR cited above, any perfect set which possesses a numerable subset everywhere dense can be set in one-to-one reciprocal continuous correspondence, with the real numbers between 0 and 1. Thus we have a continuous one-to-one correspondence of the points of any arc, and hence of any simple closed curve, with a numerical parameter, t. If a system of coördinates (x, y) has been introduced, the simple closed curve may be expressed in parameter form by defining $x(t)$ as the abscissa of the point of j that corresponds to t and $y(t)$ as the ordinate of the same point. The continuity of $x(t)$ and $y(t)$ is evident.

Regarding the conditions of definition 4 as a set of postulates for the determination of the notion, simple curve, the proposition just proved is in effect that in the presence of axioms I–VIII, XI, together with IX or a set of congruence axioms, the system of postulates is "categorical."† The conditions are also independent; i. e., each item of the definition is indispensable to the full definition. To prove this we give a list of point-sets each of which satisfies all the conditions except one. Our independence proofs apply to conditions A, B, C, D since the closed simple curve is defined in terms of the unclosed arc.

A_1. $\{P\}$ consists of one point.

*G. CANTOR *Zur Begründung der transfiniten Mengenlehre* I, Mathematische Annalen, vol. 46 (1895), p. 510.

†See vol. 5, p. 346, of these Transactions.

A_2. $\{P\}$ consists of a straight segment P_1P_2 and a point P_3 not on the straight line P_1P_2, the relation $\odot$ referring to a fixed sense on the straight line P_1P_2.

A_3. $\{P\}$ consists of two points P_1, P_2 with the conventions $P_1 \odot P_2$, $P_1 \odot P_1$, $P_2 \odot P_2$.

A_4. $\{P\}$ consists of seven points $P_1 \cdots P_7$, the relation $\odot$ being defined by the following table

$\odot$	1	2	3	4	5	6	7
1		•		•			•
2			•		•		•
3	•					•	•
4		•	•			•	
5	•		•	•			
6	•	•			•		
7				•	•	•	

B_1. $\{P\}$ consists of two points P_1 and P_2 with the convention $P_1 \odot P_2$.

B_2. $\{P\}$ consists of all the points of a straight line with one exception, $\odot$ being one of the two senses along the line.

C_1. $\{P\}$ consists of all the points of a straight line P_1P_2 with the exception of the point P_1 and the segment P_1P_2, $\odot$ being the sense from P_1 to P_2.

C_2. $\{P\}$ consists of all the points of a straight line P_1P_2 with the exception of the point P_2 and the segment P_1P_2, $\odot$ being the sense from P_1 to P_2.

D. P consists of the points of a broken line $P_1P_2P_3P_4$, where P_4 is a point of the segment P_1P_2, $\odot$ being the sense P_1P_2, and P_4 being counted as a point of P_1P_2. This case shows the necessity of condition D in theorem 2 since $\odot$ may also be the sense along the broken line $P_1P_4P_3P_2$.

§ 5. *A simple curve as a planar point set.*

DEFINITION 8. A geometrically *closed* set of points is a set that includes all its geometrical limit points.

THEOREM 3. *If* $[P]$ *is any geometrically closed set of points and a any arc that does not have any point in common with* $[P]$, *then* (1) *there exists a finite set of triangles* $\{t_n\}$ *such that every point of a is interior to at least one* t_n *and every point of* $[P]$ *is exterior to every* t_n, *and* (2) *the two end points* A_1A_2 *of a can be joined by a broken line not meeting* $[P]$.

Proof. (1) If A is any point of a there must be a triangle, t, including A and not including any point of $[P]$; otherwise A would be a limit point of $[P]$. By condition c, each of these triangles, t, determines an arc, i, of a which lies entirely within t and includes the point A to which t belongs. By

the HEINE-BOREL theorem applied to the arc a, there is a finite subset $[i_n]$ of the arcs i such that every point of a belongs to one arc i_n. The finite set of triangles, t_n, that determined these arcs i_n is the set required by conclusion (1) of the theorem.

(2) The end points of the arcs i_n constitute a finite set of points which we take as ordered by the sense of a from A_1 to A_2. The broken line* joining these points taken in order is such that each side lies within a triangle t and therefore cannot meet $[P]$.

COROLLARY. If $[P]$ is any geometrically closed set of points and Q_0 a point not of $[P]$, then Q_0 and the set of points, Q, that can be joined to Q_0 by arcs not meeting $[P]$ constitute an open region.

The following theorem is a direct consequence of definitions 4 and 5 and its proof as well as that of theorem 5 is omitted.

THEOREM 4. *About any point of a segment of a simple curve there is a triangle which includes no points of the curve not on the segment.*

In the sense of definition 8, a straight line is a geometrically closed set. A straight line, however, lacks a property possessed by any one of its intervals, namely that every infinite subset has a limit point. For this kind of set we introduce the phrase "finitely closed" because any such set can be enclosed by a finite set of triangles. This property, however, is not used and not proved in the present paper.

DEFINITION 9. A *finitely closed* set of points is a geometrically closed set of which every infinite subset possesses a geometrical limit point. A finitely closed set, every point of which is a geometrical limit point, is a *finitely perfect* set. A finitely perfect set of points which cannot consist entirely of two closed subsets is called a *coherent* set of points.†

THEOREM 5. *A closed curve or an arc of curve is a finitely perfect set of points which cannot consist entirely of two subsets, each of which includes all its limit points. In other words a closed curve or an arc of curve is a coherent set of points.*

THEOREM 6. *If every point of a coherent set of points $[A]$ is on a simple curve c, closed or unclosed, then $[A]$ is an interval of c.*

Proof. If $[A]$ were not an arc of c there must in case c is unclosed be one, and in case c is closed, two points, C_1, C_2, of C not on a which separate the points of c into two sets, c', c'' each containing points of $[A]$. Let $[A']$ denote the points common to $[A]$ and c' and $[A'']$ denote the points common to $[A]$ and c''. Every geometrical limit point of $[A']$ would be a

*This broken line of course need not be simple. A broken line with multiple points has a sense independent of the definition of sense on a simple curve. See chapter II, § 4.

†This is the "Begriff des Zusammenhangs" of JORDAN and SCHOENFLIES. Cf. SCHOENFLIES, Mathematische Annalen, vol. 58 (1903), p. 208.

geometrical limit point of $[A]$, therefore a point of $[A]$, and hence a point of c. Being a point of c and a geometrical limit point of c', by theorem 4, it would be a point of c' and hence a point of $[A']$. $[A']$ would therefore be a closed set and by parity of reasoning $[A'']$ also would be closed and thus the definition of $[A]$ would be contradicted.

Corollary. If every point of an arc, a, is on a simple curve, c, then a is an interval of c.

THEOREM 7. *If c is any simple curve, any triangle, t, of the plane includes points not on c.*

Proof. Let a be a straight line interval lying wholly within t. By theorem 6, a either contains points not on c, in which case our conclusion holds, or a is an arc of c. In the latter case, by theorem 4, a triangle, t', exists about any interior point of a including no points of c not on a. Points of the boundary of this triangle within t and not on a are not on c.

§ 6. *The approach to and crossing of a boundary.*

DEFINITION 10. Let P be an interior point of a region, R, and B a point of the boundary b of R. An arc of a curve, a, whose end points are P and B *approaches B from P through R* if every interval of a, one of whose end points is B, contains interior points of R. The approach is *one-sided* if, besides the above condition, the arc, a, contains no points exterior to R. The approach is *simple* if all the points of a, except B, are interior points of R.

An arc a' *departs from* a point B' of b *to* a point Q exterior to R if every interval of a' with B' as an end point contains points exterior to R. The departure is *one-sided* if, besides the above condition, the arc a' contains no points interior to R. The departure is *simple* if all the points of a' except B' are exterior to R.

A curve c *crosses the boundary in a point B* if, with respect to a fixed sense, B is between two points C_1, C_2 of c, C_1 interior and C_2 exterior to R, in such a way that the arc C_1B approaches B through R and BC_2 departs from B to C_2.

A curve c *crosses the boundary b in a pair of points BB'* if, with respect to a certain sense, one arc BB' of c is composed entirely of boundary points and if there are two points C_1C_2 of c such that C_1 is interior to R and an arc C_1B of c approaches B from C_1 while C_2 is exterior to R and an arc $B'C_2$ departs from B' to C_2.

The crossing of a boundary is *simple* if both the approach and departure at the point B or point pair BB' are simple.

The crossing of a straight line by a curve is a special case of the definition just given. A curve is said to cross a segment AB if the curve crosses the line AB in a point or a pair of points.

THEOREM 8. *Any simple curve joining an interior point of a region to an exterior point crosses the boundary in a point or a pair of points.*

Proof. Let I be the interior point, O the exterior point, and a any arc of the curve from I to O. Let $\{A\}$ be the set of all points, A, of the arc a such that every point following I and preceding A is an interior or boundary point of the region. There are such points because of condition C of the definition in § 3. By the ordinal continuity of a, the set $\{A\}$ has a first forward bound B, i. e., a first point in the sense from I to O that follows every point of $\{A\}$ except possibly B itself.

The arc BO of a departs from B to O as otherwise every arc BB'' of BO would contain only interior or boundary points of the region and thus B would not be a bound of $\{A\}$. Two cases can now occur. Either B is approached from I by the arc IB of a in which case our conclusion follows, or there are points A' of $\{A\}$ such that the arcs $A'B$ include only boundary points. In the last case the set of all points, A', must have a first forward bound B' in the sense from B to I. The point B' is evidently a boundary point and is approached from I by the arc of a, IB'. Thus in the second case, the boundary is crossed in the pair of points $B'B$.

THEOREM 9. *If a simple closed curve crosses a side of a polygon (simple or not) in one point or point-pair, it must pass through a vertex or cross the same or another side in another point or point-pair.*

Proof. Let the polygon be $P_1P_2\cdots P_n$ and let the curve, j, cross it in a point of P_1P_2. If there is another crossing on the segment P_1P_2 or if j passes through a vertex, $P_1\cdots P_n$, the theorem is verified. These cases disposed of, $P_1P_2P_3$ may either be collinear or non-collinear. In the first case the original crossing may have been on P_2P_3 in which case the theorem is verified or it may have been on P_1P_3 in which case we pass to the paragraph below. In case $P_1P_2P_3$ are non-collinear there must be a point J_1 of j and a point O_1 common to j and P_1P_2 such that in a certain sense on j the arc J_1O_1 of j approaches O_1 through the region on one side of P_1P_2; likewise there must be a point J_2 of j on the opposite side of P_1P_2 from J_1 and a point O_2 common to P_1J_1 and j such that in the same sense the arc O_2J_2 departs from O_2 to J_2. Moreover the points J_1 and J_2 may be so chosen that one and only one of them lies within the triangle $P_1P_2P_3$. Since j crosses P_1P_2 only once, O_1 and O_2 are on the same arc of j with end points J_1J_2. The other arc, a, of j with end points J_1J_2 must, by theorem 8, cross the boundary of the triangle $P_1P_2P_3$ and since it does not pass through a vertex, must either cross P_2P_3 verifying the theorem or cross P_1P_3. In the latter case, let O_1' be the first point in the sense from J_1 to J_2 in which a meets P_1P_3 and O_2' the last such point. Upon the arcs J_1O_1' and $O_2'J_2$ there must be two points of a, J_1' and J_2' on opposite sides of P_1P_3 such that in opposite senses along j the arcs $J_1'O_1'$ and $J_2'O_2'$ approach O_1' and O_2'

from opposite sides of P_1P_3. In case $P_1P_3P_4$ are non-collinear J_1' and J_2' may be so chosen that one is interior and the other exterior to the triangle $P_1P_3P_4$.

Thus whether $P_1P_3P_4$ are or are not collinear we proceed as with $P_1P_2P_3$, either verifying the theorem or arriving at the case $P_1P_4P_5$. Continuing this process, by a finite number of steps we come to $P_1P_{n-1}P_n$ and verify the theorem if it is not fulfilled at one of the intermediate steps.

COROLLARY 1. If j_1 is a simple closed curve having an arc which is a linear interval J_1J_2, and if the segment J_1J_2 is crossed by a simple closed curve j_2 in one point or point pair, then either J_1J_2 is crossed in another point or point pair or the non-linear arc J_1J_2 of j_1 has a point in common with j_2.

Proof. In case J_1J_2 were not crossed more than once and the other arc J_1J_2 of j_1 did not meet j_2, by theorem 3 J_1 and J_2 could be joined by a broken line not meeting j_2 and we should thus have a contradiction with theorem 9.

COROLLARY 2. Any simple closed curve j_1 having a linear arc J_1J_2 decomposes its plane into at least two regions.

Proof. Let PQ be a linear segment crossing J_1J_2 in a point O. The region composed of all points that can be joined to P by broken lines not meeting j_1 is by theorem 9 separated from the region similarly connected with Q.

LEMMA A. *Any simple closed curve j decomposes the plane in which it lies into at least two regions.*

Proof. Let J_1 and J_2 be two points of j such that the linear segment J_1J_2 has no point in common with j. Such points J_1J_2 exist, for if a is any line joining two points of j, it either has an interval free of j points and whose endpoints are the required points J_1J_2 or its points in common with j constitute a single arc of j (theorem 6, corollary). In the latter case any line a' joining a point of j on a to a point of j not on a evidently has the required points J_1J_2.

Let t be a triangle about J_1 such that one of its sides meets the linear segment J_1J_2 in a point O. Let Q' and Q'' be two points of this side separated by O and such that the linear interval $Q'Q''$ contains no point of j. The existence of these points depends on the theorem that j is a geometrically perfect set.

J_1 and J_2 decompose j into two segments which with the linear interval J_1J_2 constitute two closed curves j' and j''. Assign the notation so that the first point, J_1', after Q'' in the sense $Q'OQ''$ in which the boundary of t meets j shall be a point of j'. It follows that the first point J_1'' after Q' in the sense $Q''OQ'$ in which the boundary of t meets j is a point of j''. For if it were a point of j', the closed curve composed of the boundary of t from J_1'' to J_1' in the sense $Q'OQ''$ and the arc common to j and j' between J_1' and J_1'' would cross the linear segment J_1J_2 of j'' simply in O and would meet j'' in no other point. This would contradict corollary 1, theorem 9.

Thus J_1'' is a point of j''. Let J_0'' be the first point after J_1' in the sense $Q'OQ''$ in which the boundary of t meets j''. By the continuity of j, there

exists a segment of the boundary of t just preceding J_0'' in the sense $Q'OQ''$ and containing no point of j' or j''. Let X be any point of this segment. The broken line b'' composed of the boundary of t in the sense $Q'OQ''$ from Q'' to X does not meet j''. Likewise X is joined to Q' by a simple curve c' composed of the linear segment XJ_0'', the common part of j'' and j from J_0'' to J_1''* and the part of the boundary of t from J_1'' to Q' in the sense $Q'OQ''$. Thus c' cannot meet j' and, applying theorem 3, c' can be replaced by a broken line b' joining X to Q' without meeting j'. We are now ready to complete the proof of our lemma by showing that X cannot be joined to O by a broken line not meeting j.

In the sense from X to O any such broken line would meet the linear segments J_1J_2 and $Q'Q''$ in some first point O_1. If O_1 were on J_1J_2, some point S preceding O_1 in the sense from X to O could be joined to a point B of $Q'Q''$ by a segment not meeting j' or j''. Call b the resulting broken line from X to B. In case O_1 were not on J_1J_2 it would be on $Q'Q''$ and different from O, and b would be the broken line from X to $O_1 = B$.

If B were on the same side of the line J_1J_2 with Q'' then the polygon composed of b and b' and BQ' would be crossed by j' in O and would meet j' in no other point, contradicting theorem 9. If B were on the opposite side of the line J_1J_2 from Q'' the polygon composed of b and b'' and BQ'' would be crossed by j'' in O and would meet j'' in no other point. X and O are therefore two points that cannot be joined by a broken line not meeting j.

§ 7. *Finite accessibility.*

DEFINITION 11. A point C of a curve c is *finitely accessible* from a point P not on c if there is a broken line from C to P not meeting c except in C.

LEMMA B. *If P is a point not on a simple closed curve j, and J_1 and J_3 are any two points of j finitely accessible from P or limit points† of the points finitely accessible from P, then there exists a pair of points J_2 and J_4 finitely accessible from P that separate J_1 and J_3.*

Proof. Let t_1 be a triangle about J_1 not including J_3, and t_3 a triangle about J_3 not including any point of t_1. By condition C of the definition of j, there is a segment of j including J_1 and lying wholly within t_1; by theorem 4 there is a triangle t_1' about J_1 within t_1 and including no point of j not on this segment. Thus every segment of j with end points on t_1 which meet t_1' must include J_1. Similarly there is within t_3 a triangle t_3' such that every segment of j with end points on t_3 which meets t_3' must include J_3.

*Of course it may happen that $J_0'' = J_1''$. In this case c' is a broken line.

†On a simple closed curve the notions of ordinal and geometrical limit points are interchangable: therefore we drop the distinction.

Let J_1' be a point finitely accessible from P within t_1' and J_3' a point finitely accessible from P within t_3'. The points J_1' and J_3' are thus joined by a broken line b, meeting j only in J_1' and J_3', which without loss of generality may be supposed simple. On this broken line let P_1 be the first point in the sense from J_3' to J_1' in which it meets the boundary of t_1. P_1 lies on an interval i_1 of the boundary of t_1 containing no points of j but such that its end points are points of j. Let P_2 be the last point in the sense from J_3' to J_1' in which b meets the interval i_1. In case P_2 is distinct from P_1 replace the portion of the broken line from P_1 to P_2 by the portion of i_1 from P_1 to P_2, calling the new broken line b_1. If b_1 crosses the interval i_1, J_2 and J_4 are the end points of the interval. If b_1 does not cross i_1 there must be some point P_3 beyond P_2 in the sense from J_3' to J_1' in which b_1 meets the boundary of t. The point P_3 must lie on an interval i_3 of the boundary of t_1 analogous to i_1. Proceed with i_3 as with i_1. Since J_1' is inside t_1 and J_3' outside t_1 and since b has but a finite number of sides, we must by repeating the process above come to a *first* interval i_k, in which the boundary of t_1 is crossed by a reduced broken line b_k from J_3' to J_1' in a point P_k or a point pair P_kP_{k+1}. The end points of the j-point free interval i_k of the boundary of t_1 are now to be shown to be the required J_2 and J_4.

We prove first that J_2 and J_4 separate J_3' and J_1'. If this were not so, let the simple closed curve formed by b_k and the arc $J_1'J_3'$ of j not including J_2 and J_4 be denoted by j_b. Also let j_i denote the simple closed curve formed by i_k and the arc J_2J_4 of j not including J_3' and J_1'. The simple closed curve j_b would cross the arc i_k of j_i in the point P_k or point pair P_kP_{k+1} and would meet j_i in no other point, contrary to corollary 1, theorem 9.

Hence J_1' and J_3' are on different arcs of j with end points J_2 and J_4. But by the construction of the triangle t_1', J_1 must be on the same arc with J_1' and by the construction of t_3', J_3 must be on the same arc with J_3'. Hence J_2J_4 separate J_1J_3.

THEOREM 10. *The set of points of a simple curve j finitely accessible from a point* P *not on j is everywhere dense on j.*

Proof. Denote by $[J]$ the set of points of j which are either finitely accessible from P or are limit points of the set of finitely accessible points. The theorem amounts to showing that $[J']$ is identical with j. But if any point J_0 of j should not belong to $[J']$ it would lie on an arc of j free of points J' and having two points of $[J']$ as end points. This would contradict lemma B.

§ 8. *Decomposition of a plane by a simple closed curve.*

LEMMA *C*. Any simple closed curve of which one arc is a linear interval decomposes its plane into two open regions.

Proof. It has been shown (corollary 2, theorem 9) that j decomposes the plane into at least two regions. The regions are open because a supposed frontier point of the set of points $[P]$ that can be joined to a point P_0 not on j could, if not itself a point of j, be surrounded by a triangle not meeting j and containing points of $[P]$; it would therefore be an interior point of $[P]$, contrary to hypothesis.

By theorem 10 every point O of the straight arc of j is finitely accessible from any point of the plane. Thus if there were three distinct regions there would be three segments meeting in O and one lying in each of the three regions. But as two of these must lie on the same side of the straight segment of j they could be joined by a straight segment not meeting j, contrary to the hypothesis that the three regions are separated from one another by j. Hence j decomposes the plane into two and only two open regions.

THEOREM 11. *Every simple closed curve, j, decomposes its plane into two open regions.*

Proof. By lemma *A* the curve decomposes the plane into at least two regions which by the reasoning of the first paragraph of the proof of lemma *C* are open regions. Let P be any point not on j and let PJ_1 and PJ_2 be two linear intervals meeting j only in J_1 and J_2. J_1 and J_2 exist because j is a perfect set of points. Let Q be any point not on j and not in the same region with P and let J_3 be a point on j such that the linear segment QJ_3 does not meet j and such that J_3 is distinct from J_1 and J_2. Then QJ_3 does not meet PJ_1 or PJ_2 and Q can by theorem 10 be joined by a broken line not meeting PJ_1, PJ_2, QJ_3, or j except in J_4 to a point J_4 of j in the order $J_1J_2J_3J_4$. The broken line J_1PJ_2, the points between J_2 and J_3 in the sense $J_1J_2J_3$, the broken line J_3QJ_4 and the points between J_4 and J_1 in the sense $J_1J_2J_3$ constitute a simple closed curve j' of the type which we have proved to decompose the plane into two and only two regions. The points of the segments J_1J_2 and J_3J_4 in the sense $J_1J_2J_3$, are not points of j' and must lie both in the same region or in opposite regions with respect to j'. If they were in the same region a point in the region not containing the segments J_1J_2 and J_3J_4 could by theorem 10 be joined by broken lines not meeting j to P and Q, thus contradicting the hypothesis that P and Q are in different regions.

Having shown that the arcs J_1J_2 and J_3J_4 (in the fixed sense $J_1J_2J_3$) are in opposite regions with respect to j' we are ready to complete the proof that j does not decompose the plane into more than two regions. A point R in a sup-

posed third region could be joined because of theorem 10 by a broken line not meeting j except in its end-point to a point J_5 of J_1J_2 and by a similar broken line to a point J_6 of J_3J_4. Since R would not be in the same region with P or Q these broken lines would not meet the broken line part of j'. Thus we should have two points J_5 and J_6 in opposite regions with respect to j' joined by a broken line not meeting j' contrary to lemma C. Hence j decomposes the plane into not more than two, and therefore into exactly two, open regions.